Telindus 1031 Router

Telindus 1031 Router

User and reference manual

Version: 1.1 181341

Telindus Technical Publications – Geldenaaksebaan 335 - B-3001 Leuven - Belgium – Tel. +32 16 382011

Document properties

Subject	Telindus 1031 Router
Manual type	User and reference manual
Version	1.1
Code	181341
Modification date	21 October 2002 ©Telindus

Copyright notice

The information and descriptions contained in this publication are the property of Telindus. Such information and descriptions must not be copied or reproduced by any means, or disseminated or distributed without the express prior written permission of Telindus.

This publication could include technical inaccuracies or typographical errors, for which Telindus never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new editions of this publication. Telindus may make improvements and/or changes in the product(s) described in this publication at any time, without prior notice.

Safety requirements

Carefully read the safety instructions at the beginning of 2 - Installing and connecting the Telindus 1031 Router on page 13.

The connectors of the Telindus 1031 Router should only be connected to the following circuit types:

Connector name	Connector label	Connector type	Circuit type
LAN connector	LAN	RJ45	SELV
G703 interface connector	G703	RJ45	SELV
auxiliary connector	AUX (DTE)	subD-9	SELV
control connector	CTRL (DCE)	subD-9	SELV

- SELV (Safety Extra Low Voltage): local connection (e.g. PC to Telindus 1031 Router) or leased line inside the building.
- TNV-1 (Telecom Network Voltage): leased line outside the building.
- TNV-2: PSTN from PABX inside the building.
- TNV-3: PSTN from operator PABX outside the building.

Statements

CE

http://www.telindusproducts.com → Products → Choose a product → Download certificates

Hereby, Telindus declares that this Telindus 1031 Router complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Hierbij verklaart Telindus dat deze Telindus 1031 Router overeenstemt met de essentiële vereisten en andere relevante bepalingen van Richtlijn 1999/5/EC.

Par la présente, Telindus déclare que ce Telindus 1031 Router est en conformité avec les exigences essentielles et autres articles applicables de la Directive 1999/5/EC.

Hiermit, Telindus erklärt daß dieser Telindus 1031 Router in Fügsamkeit ist mit den wesentlichen Anforderungen und anderen relevanten Bereitstellungen von Direktive 1999/5/EC.

Mediante la presente, Telindus declara que el Telindus 1031 Router cumple con los requisitos esenciales y las demás prescripciones relevantes de la Directiva 1999/5/CE.

A Telindus declara que o Telindus 1031 Router cumpre os principais requisitos e outras disposições da Directiva 1999/5/EC.

Col presente, Telindus dichiara che questo Telindus 1031 Router è in acquiescenza coi requisiti essenziali e stipulazioni attinenti ed altre di Direttivo 1999/5/EC.

Με το παρον, η Telindus δηλωνει οτι αυτο το Telindus 1031 Router ειναι συμμορφουμενο με τιζ βασικεζ απαιτησειζ και με τιζ υπολοιπεζ σχετικεζ διαταξειζ τηζ οδηγιαζ 1999/5/EC.

Organisation of this manual

This manual contains the following main parts:

Part	This part …
User manual	shows you how to install and connect the Telindus 1031 Router. It also gives a basic configuration of the Telindus 1031 Router.
Reference manual	gives more detailed information on the Telindus 1031 Router. It contains a complete description of all the configuration, status, performance and alarm parameters for look-up purposes.
Annex	gives additional information.

Refer to the Table of contents on page vii for a detailed overview of this manual.

Application software version

This manual describes the features, containment tree and attributes of the Telindus 1031 Router application software version T2802/00200.

Audience

This manual is intended for computer-literate people, who have a working knowledge of computing and networking principles.

Your feedback

Your satisfaction about this purchase is an extremely important priority to all of us at Telindus. Accordingly, all electronic, functional and cosmetic aspects of this new unit have been carefully and thoroughly tested and inspected. If any fault is found with this unit or should you have any other quality-related comment concerning this delivery, please submit the Quality Comment Form on our web page at http://www.telindusproducts.com/quality.

Typographical conventions

The following typographical conventions are used in this manual:

The format ...	indicates ...
Normal	normal text.
Italic	• new or emphasised words • application windows, buttons and fields. E.g. In the *File name* field enter ...
`Computer`	text you have to enter at the DOS or CLI prompt, computer output and code examples. E.g. `NOK,1,1,Invalid command.`

`Computer Bold`	text you have to enter at the DOS or CLI prompt when it is part of a mix of computer input and output.
	E.g.
	`/o1003:"Edit Configuration"`
	`>`**`get sysName`**
	`  sysName = "Orchid 1003 LAN"`
	`/o1003:"Edit Configuration"`
	`>`

Narrow	containment tree objects and attributes of a device when they are mentioned in the normal text. I.e. when they are not a part of computer input or output. E.g. Use the sysName attribute in order to ...
Blue	references to other parts in the manual. E.g. Refer to xx - Title for more information.
Blue underline	• a hyperlink to a web site. E.g. http://www.telindus.com • a reference to another manual. E.g. Refer to the TMA manual for …

Graphical conventions

The following icons are used in this manual:

Icon	Name	This icon indicates …
	Remark	remarks or useful tips.
	Caution	text to be read carefully in order to avoid damage to the device.
	Warning	text to be read carefully in order to avoid injury.
	DIP switch	a DIP switch or strap table.
	Basic attribute	a basic attribute in the containment tree of the Telindus 1031 Router.
	Advanced attribute	an advanced attribute in the containment tree of the Telindus 1031 Router.
	Structured attribute	a structured attribute within another attribute in the containment tree of the Telindus 1031 Router.
	Action	an action in the containment tree of the Telindus 1031 Router.

Table of contents

User manual 1

1 Introducing the Telindus 1031 Router 3
1.1 What is the Telindus 1031 Router? 4
1.2 Telindus 1031 Router applications 5
1.3 Telindus 1030 Router family overview 6
1.4 Management tools 10
1.5 Management tools connection possibilities 12

2 Installing and connecting the Telindus 1031 Router 13
2.1 Safety instructions 14
2.2 Unpacking 15
2.3 Selecting a site 16
2.4 Installation and connection precautions 17
2.5 Connecting the Telindus 1031 Router 18
2.6 The front panel LED indicators 24

3 DIP switches of the Telindus 1031 Router 29
3.1 The Telindus 1031 Router motherboard 30
3.2 DIP switches of the Telindus 1031 Router 31
3.3 Opening and closing the housing 32

4 Managing the Telindus 1031 Router 33
4.1 Managing the Telindus 1031 Router with TMA 34
4.2 Introducing the management terminology 40
4.3 The objects in the Telindus 1031 Router containment tree 44
4.4 Adding an object to the containment tree 45
4.5 Telindus 1031 Router attribute overview 50

5 Basic configuration 51
5.1 Reading DIP switch tables and TMA attribute strings 52
5.2 Configuring IP addresses 55
5.3 Configuring the G703 interface 61
5.4 Configuring passwords 62
5.5 Configuring the major features of the Telindus 1031 Router 65
5.6 Executing configuration actions 66

6 Configuring the WAN encapsulation protocols 71
6.1 Selecting a WAN encapsulation protocol 72
6.2 Configuring PPP encapsulation 73
6.3 Configuring Frame Relay encapsulation 77
6.4 Configuring ATM encapsulation 86
6.5 Configuring HDLC encapsulation 95

7 Configuring the router 97
7.1 Introducing routing 98
7.2 Configuring static routes 100
7.3 Configuring the Routing Information Protocol 107
7.4 Configuring address translation 116
7.5 Configuring L2TP tunnelling 127
7.6 Configuring traffic and priority policy on the router 130
7.7 Configuring an extended access list 138

8 Configuring the bridge 139
8.1 Introducing bridging 140
8.2 The self-learning and Transparent Spanning Tree bridge 141
8.3 The Spanning Tree root bridge 142
8.4 The Spanning Tree topology 143
8.5 The Spanning Tree bridge port states 144
8.6 The Spanning Tree Bridge Protocol Data Unit 145
8.7 The Spanning Tree behaviour 146
8.8 The Spanning Tree priority and cost 147
8.9 Configuring bridging 149
8.10 Configuring traffic and priority policy on the bridge 154

9 Configuration examples 159
9.1 LAN extension over a PDH/SDH network 160
9.2 LAN extension over a Frame Relay network 161
9.3 LAN extension over an ATM network 162
9.4 Connecting a LAN to the Internet using NAT and PAT 163
9.5 Using PAT over PPP with a minimum of official IP addresses 164
9.6 Combining bridging and routing in a network 165
9.7 Connecting two networks through a tunnel 166
9.8 Connecting VLAN enabled switches over a WAN 168

Reference manual 169

10 Configuration attributes 171
10.1 Configuration attribute overview 172
10.2 General configuration attributes 174
10.3 LAN interface configuration attributes 178
10.4 WAN interface configuration attributes 181
10.5 Router configuration attributes 200
10.6 Bridge configuration attributes 231
10.7 SNMP configuration attributes 238
10.8 Management configuration attributes 240
10.9 Proxy configuration attributes 244

11 Status attributes 245
11.1 Status attribute overview 246
11.2 General status attributes 248
11.3 LAN interface status attributes 251
11.4 WAN interface status attributes 257
11.5 Router status attributes 273
11.6 Bridge status attributes 287
11.7 Management status attributes 293
11.8 File system status attributes 294
11.9 Operating system status attributes 296
11.10 Proxy status attributes 297

12 Performance attributes 299
12.1 Performance attributes overview 300
12.2 LAN interface performance attributes 302
12.3 WAN interface performance attributes 305
12.4 Router performance attributes 312
12.5 Bridge performance attributes 318
12.6 Management performance attributes 321
12.7 Operating system performance attributes 323
12.8 Proxy performance attributes 325

13 Alarm attributes 327
13.1 Alarm attributes overview 328
13.2 Introducing the alarm attributes 329
13.3 General alarms 332
13.4 LAN interface alarms 334
13.5 G703 interface alarms 335
13.6 G703 channel alarms 336
13.7 Router alarms 337

14 TMA sub-system picture 339

15 Auto installing the Telindus 1031 Router 341
15.1 What is BootP and DHCP? 342
15.2 Getting the LAN IP address 343
15.3 Getting the configuration with TFTP 344
15.4 Creating configuration files 347
15.5 Creating a binary configuration file 348
15.6 Creating an ASCII configuration file 349

16 Downloading software 353
16.1 What is boot, loader and application software? 354
16.2 Downloading application software using TMA 355
16.3 Downloading application software using TFTP 356
16.4 Downloading application or loader software using TML 357
16.5 Downloading application or loader software in loader mode 358
16.6 Downloading files to the file system 359

17 Technical specifications 361
17.1 G703 interface specifications 362
17.2 LAN interface specifications 363
17.3 Control connector specifications 364
17.4 Auxiliary connector specifications 365
17.5 ATM encapsulation specifications 366
17.6 Frame Relay encapsulation specifications 366
17.7 PPP encapsulation specifications 366
17.8 IP routing specifications 367
17.9 Bridging specifications 367
17.10 Routing and bridging performance specifications 367
17.11 Power requirements 368
17.12 Dimensions 368
17.13 Safety compliance 368
17.14 Over-voltage and over-current protection compliance 368
17.15 EMC compliance 368
17.16 Environmental compliance 369

Annex 371

Annex A:common TCP and UDP numbers 373

Annex B:product information 375

Index 377

User manual

1 Introducing the Telindus 1031 Router

This chapter gives an introduction to the Telindus 1031 Router. The following gives an overview of this chapter:

- 1.1 - What is the Telindus 1031 Router? on page 4
- 1.2 - Telindus 1031 Router applications on page 5
- 1.3 - Telindus 1030 Router family overview on page 6
- 1.4 - Management tools on page 10
- 1.5 - Management tools connection possibilities on page 12

1.1 What is the Telindus 1031 Router?

The Telindus 1030 Router series is a set of IP access routers designed for high-speed WAN access. They offer high performance IP routing and bridging.

The versions with 2Mbps E1 interfaces are extremely well suited to transport LAN traffic over a PDH or SDH backbone network. These G703 interfaces (1 or 2, depending on the model) can be used as channelised E1 interfaces, offering multiple logical interfaces on one physical port. The versions with serial interface (X.21, V.35, V.36, RS530 or RS530A) allow speeds up to 10Mbps.

The Telindus 1030 Router series can directly encapsulate the LAN traffic for transmission over ATM and frame relay WAN networks. ATM encapsulation includes RFC2684 (formerly RFC1483), PPP over ATM, and PPP over Ethernet and RBE (Routed Bridge Encapsulation). For point to point set-ups and connections over PDH or SDH networks, PPP can also be used as the WAN protocol. Additionally, the Telindus 1030 Router series is equipped with an AUX V.24 WAN interface for low-speed asynchronous PPP connections and a control V.24 management interface.

The Telindus 1030 Router series supports differentiated services based on VPNs (Virtual Private Networks). Therefore it integrates features like L2TP (Layer 2 Tunnelling Protocol), IPSEC, 802.1Q (VLAN tagging) and COS (Class Of Service) based on Diffserv priority tagging and queuing. A specific model supporting DES and 3DES encryption is also available.

The Telindus 1030 Router series is designed for integration into demanding network environments and can be controlled by a complete set of network maintenance and management tools. It supports auto-install features over the WAN network. This makes it ideally suited for plug-and-play installation at customer premises while the configuration is prepared at a central site.

What is more, the Telindus 1030 Router series themselves are designed to act as a management concentrator (also called management proxy).

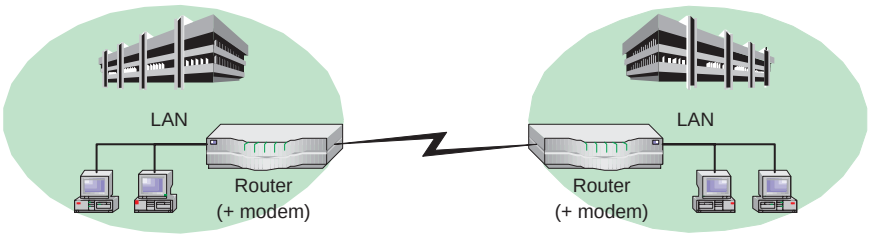
Refer to 1.3 - Telindus 1030 Router family overview on page 6 for a detailed description of the differences between the models of the Telindus 1030 Router series.

1.2 Telindus 1031 Router applications

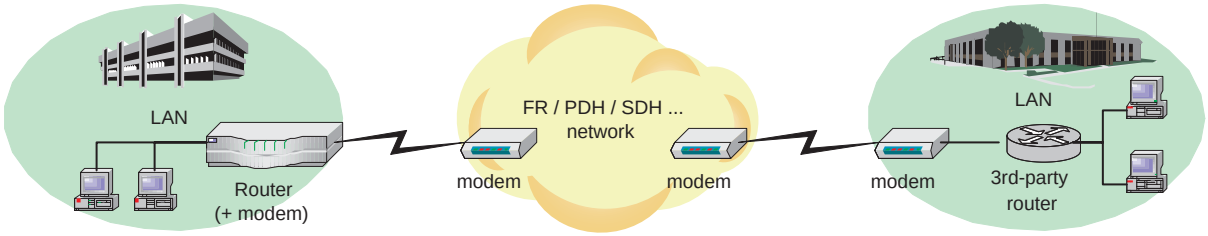
Some examples of Telindus 1031 Router applications are:

- LAN to LAN connection over a line
- LAN extension over a network
- LAN to Internet connection
- LAN to network connection while managing the local access devices

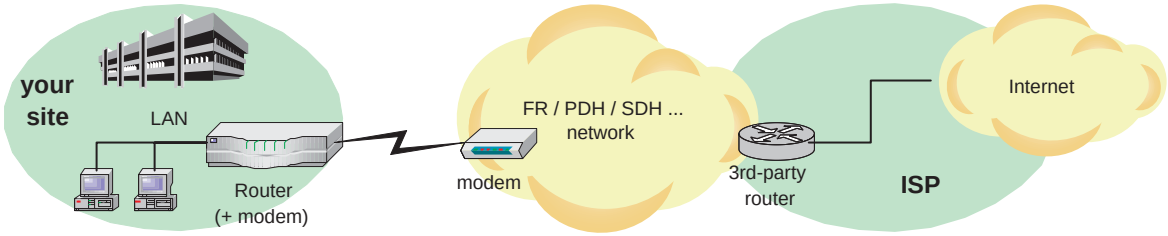
Point-to-point LAN interconnection



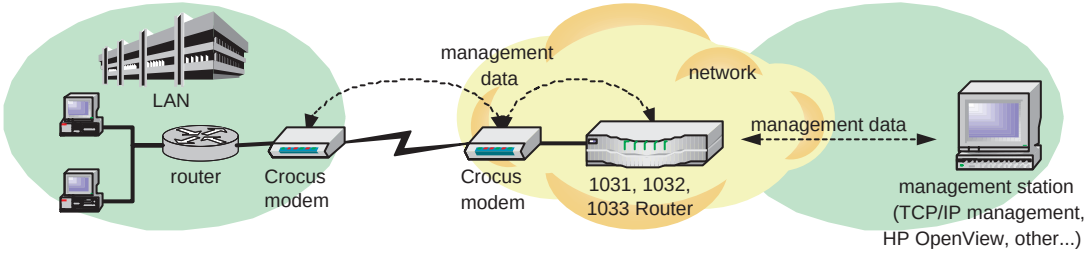
LAN extension over a network



LAN to Internet connection



LAN to network with local management



1.3 Telindus 1030 Router family overview

The Telindus 1030 Router family is a range of routers each with their own specific features. This section gives an overview of all the members of the Telindus 1030 Router family. First this section shows you how to distinguish the different members from one another. Then it lists the features that apply on the complete Telindus 1030 Router family. Finally, this section highlights the specific features of each member of the Telindus 1030 Router family.

The following gives an overview of this section:

- 1.3.1 - How to distinguish the different members of the Telindus 1030 Router family? on page 7
- 1.3.2 - Common Telindus 1030 Router family features on page 7
- 1.3.3 - Telindus 1031 Router features on page 8
- 1.3.4 - Telindus 1032 Router features on page 8
- 1.3.5 - Telindus 1033 Router features on page 9

1.3.1 How to distinguish the different members of the Telindus 1030 Router family?

Every router of the Telindus 1030 Router family has the same front panel. The only way to distinguish them from one another is by looking at the back panel. These are displayed in the following sections.

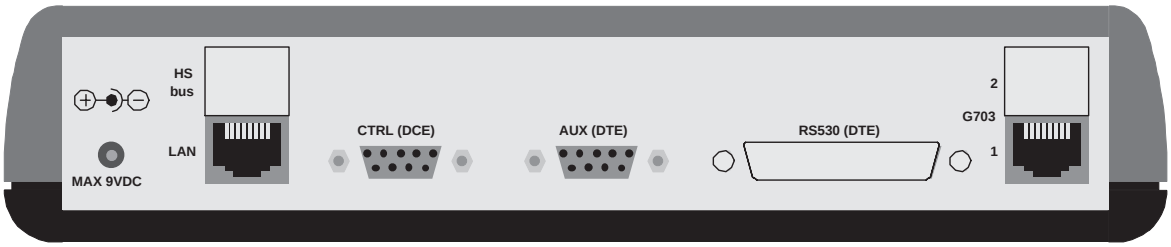
1.3.2 Common Telindus 1030 Router family features

The major features that apply on all the members of the Telindus 1030 Router family are:

- high performance routing and bridging,
- encapsulation of LAN traffic for transmission over a WAN network,
- support of differentiated services based on VPNs,
- controllable by a wide set of management tools,
- a control connector (CTRL) to connect various management tools to the 1030 Router locally (e.g. TMA, CLI, EasyConnect, etc.) or to connect Telindus devices that have to be managed by the 1030 Router (i.e. the 1030 Router as management concentrator),
- an auxiliary connector (AUX) to connect Telindus devices that have to be managed by the 1030 Router (i.e. the 1030 Router as management concentrator).

1.3.3 Telindus 1031 Router features

The following displays the back panel of the Telindus 1031 Router:

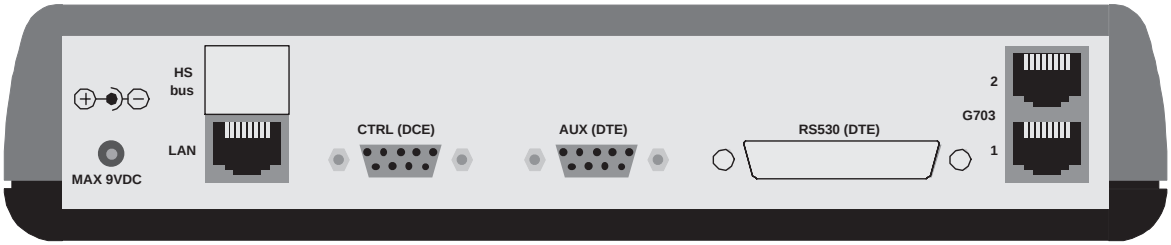


The specific features of the Telindus 1031 Router are:

- one G703 interface. This interface can be used as channelised E1 interface, offering multiple logical interfaces on one physical port.
- management concentrator capabilities. These are limited because only the CTRL and AUX connectors can be used to connect to other Telindus devices.

1.3.4 Telindus 1032 Router features

The following displays the back panel of the Telindus 1032 Router:

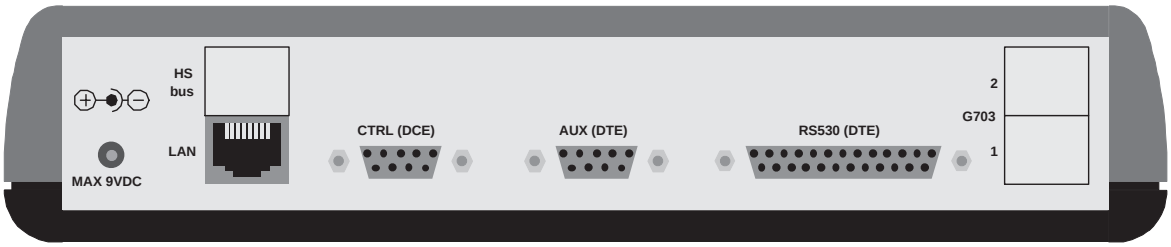


The specific features of the Telindus 1032 Router are:

- two G703 interfaces. These interfaces can be used as channelised E1 interfaces, offering multiple logical interfaces on one physical port.
- management concentrator capabilities. These are limited because only the CTRL and AUX connectors can be used to connect to other Telindus devices.

1.3.5 Telindus 1033 Router features

The following displays the back panel of the Telindus 1033 Router:



The specific features of the Telindus 1033 Router are:

- one RS530 interface. This serial interface allows speeds up to 10 Mbps. The interface can also be used as RS530A, V.35, V.36 or X.21 interface by setting the correct straps and using the correct conversion cables.
- management concentrator capabilities. These are limited because only the CTRL and AUX connectors can be used to connect to other Telindus devices.

1.4 Management tools

The Telindus 1031 Router is manageable in many different ways. This section gives a quick overview of the various management tools.

Management tool	Description and reference
TMA	TMA (Telindus Management Application) is a free Windows software package that enables you to manage the Telindus products completely. I.e. to access their configuration attributes and look at status, performance and alarm information. Refer to 4 - Managing the Telindus 1031 Router on page 33 and the TMA manual for more information.
TMA for HP OpenView	TMA for HP OpenView is the management application that runs on the widely spread network management platform HP OpenView. It offers the combination of the easy to use graphical interface of the stand-alone version of TMA, together with the advantages and features of HP OpenView. Refer to the TMA for HP OpenView manual for more information.
TMA CLI	TMA CLI (TMA Command Line Interface) enables you to use its commands in scripts in order to automate management actions. This is particularly useful in large networks. TMA CLI is a complementary product to TMA and TMA for HP OpenView. Refer to the TMA CLI manual for more information.
ATWIN	ATWIN is a menu-driven user interface. You can read and change all attributes as with TMA, but in a more basic, textual representation using a VT100 terminal. Refer to the Maintenance Tools manual for more information.
CLI	CLI is also a Command Line Interface, although not so extensive as TMA CLI. Experienced users who are familiar with the syntax can access the Telindus devices more quickly than with TMA or ATWIN. Refer to the Maintenance Tools manual for more information.
Web Interface	The Web Interface is an ATWIN alike menu-driven user interface. You can read and change all attributes as with TMA, but in a more basic representation using a web browser. Refer to the Maintenance Tools manual for more information.
EasyConnect terminal	Connecting the Telindus EasyConnect hand-held terminal through the control connector to the Telindus 1031 Router, allows you to manage the Telindus 1031 Router in a basic way using the LCD display and keyboard. This is called keyboard management. Refer to the EasyConnect manual for more information.

Management tool	Description and reference
SNMP	You can manage the Telindus 1031 Router through SNMP using any SNMP browser. The Telindus 1031 Router supports MIB2 and a private MIB, including traps. The private MIB comes with your copy of TMA. After installation of the TMA data files, the private MIB file is available in directory *C:\Program Files\TMA\snmp*[1] with the name *<filename>.mib*[2]. Refer to 10.7 - SNMP configuration attributes on page 238 and the documentation of your SNMP browser for more information.

1. The first part of the directory path may be different if you did not choose the default path during the installation of the TMA data files.
2. The filename is product dependent. To determine which MIB file corresponds with which product, refer to the *models.nms* file (located in *C:\Program Files\TMA\model*[1]).

1.5 Management tools connection possibilities

The following table gives an overview of all the management tools and how you can connect them with the Telindus 1031 Router:

Management tool	PC - Telindus 1031 Router connection		PC - management concentrator connection[1]	
	Serial[2]	IP[3]	Serial[2]	IP[3]
EasyConnect	X		X	
CLI	X[4]	X[5]	X[4]	X[5]
ATWIN	X[4]	X[5]	X[4]	X[5]
TMA	X	X	X	X
TMA CLI	X	X	X	X
TMA for HPOV		X		X
SNMP[6]		X		X
Web Interface[7]		X		X

1. Examples of management concentrators are the Orchid 1003 LAN and the Telindus 1030 Router series. Refer to their corresponding manuals for more information on how to set these devices up as management proxy.
2. A serial connection is a connection between the COM port of your PC and the control connector of the Telindus 1031 Router using a male-female DB9 cable.
3. An IP connection is a connection between your PC and the Telindus 1031 Router over an IP network.
4. Using a VT100 terminal (emulation program).
5. Using Telnet.
6. Using an SNMP browser.
7. Using a web browser.

2 Installing and connecting the Telindus 1031 Router

First this chapter gives some important safety instructions. Then it explains how to install and connect the Telindus 1031 Router.

You are advised to read this chapter from the beginning to the end, without skipping any part. By doing so, your Telindus 1031 Router will be completely installed and ready for configuration when you reach the end of this chapter.

The following gives an overview of this chapter:

- 2.1 - Safety instructions on page 14
- 2.2 - Unpacking on page 15
- 2.3 - Selecting a site on page 16
- 2.4 - Installation and connection precautions on page 17
- 2.5 - Connecting the Telindus 1031 Router on page 18
- 2.6 - The front panel LED indicators on page 24

2.1 Safety instructions

IMPORTANT SAFETY INSTRUCTIONS

Disconnect the power supply before installing, adjusting or servicing the unit.

ACHTUNG! WICHTIGE SICHERHEITSINSTRUKTIONEN

Vor sämtlichen Arbeiten am Gerät (Installation, Einstellungen, Reparaturen etc.) sollten Sie den Netzstecker aus der Steckdose ziehen.

SAFETY WARNING

To avoid damage to the unit, please observe all procedures described in this chapter.

SICHERHEITSBESTIMMUNGEN

Um eine Beschädigung des Gerätes zu verhindern, beachten Sie bitte unbedingt die Sicherheitsbestimmungen, die in diesem Abschnitt beschrieben werden.

Ensure that the unit and its connected equipment all use the same AC power and ground, to reduce noise interference and possible safety hazards caused by differences in ground or earth potentials.

2.2 Unpacking

Checking the shipping carton

Rough handling during shipping causes most early failures. Before installation, check the shipping carton for signs of damage:

- If the carton box is damaged, please place a claim with the carrier company immediately.
- If the carton box is undamaged, do not dispose of it in case you need to store the unit or ship it in the future.

Package contents

The box should contain the following items:

- Telindus 1031 Router
- TMA CD-ROM (including this User and Reference manual in PDF format)

Optionally (depending which sales item you ordered):

- external power supply with power cord (2 meter)

2.3 Selecting a site

WARNING

Always place the unit on its feet without blocking the air vents.

Do not stack multiple units directly onto each other, as stacking can cause heat build-up that could damage the equipment.

ACHTUNG

Stellen Sie das Gerät niemals seitlich, sondern nur auf den Füßen auf und achten Sie darauf, daß die Lüftungsschlitze an der Seitenverkleidung frei bleiben.

Stapeln Sie nicht mehrere Geräte direkt übereinander, dies kann zu einem Hitzestau führen.

Install the unit in an area free of extreme temperatures, humidity, shock and vibration. Position it so that you can easily see and access the front panel and its control indicators. Leave enough clearance at the back for cables and wires. Position the unit within the correct distances for the different accesses and within 2m of a power outlet.

2.4 Installation and connection precautions

ESD WARNING

The circuit boards are sensitive to electrostatic discharges (ESD) and should be handled with care. It is advisable to ensure an optimal electrical contact between yourself, the working area and a safety ground before touching any circuit board. Take special care not to touch any component or connector on the circuit board.

EMC WARNING

EMC compliant installation

The Telindus access products are fully EMC compliant. To ensure compliance with EMC directive 89/336/EEC, shielded cables or ferrite beads have to be used.

NOTE

This unit may be powered by an IT power system.

ANMERKUNG

Das Gerät kann gespeist wurden durch ein IT power System.

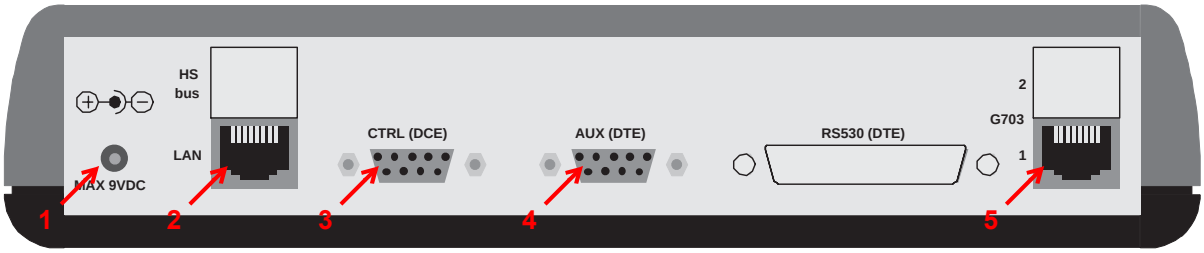
2.5 Connecting the Telindus 1031 Router

This section explains how to connect the Telindus 1031 Router. The following gives an overview of this section:

- 2.5.1 - Rear view of the Telindus 1031 Router on page 19
- 2.5.2 - Connecting the different parts of the Telindus 1031 Router on page 20
- 2.5.3 - Connecting the Telindus 1031 Router - an example on page 22

2.5.1 Rear view of the Telindus 1031 Router

The following is a rear view of the Telindus 1031 Router:



2.5.2 Connecting the different parts of the Telindus 1031 Router

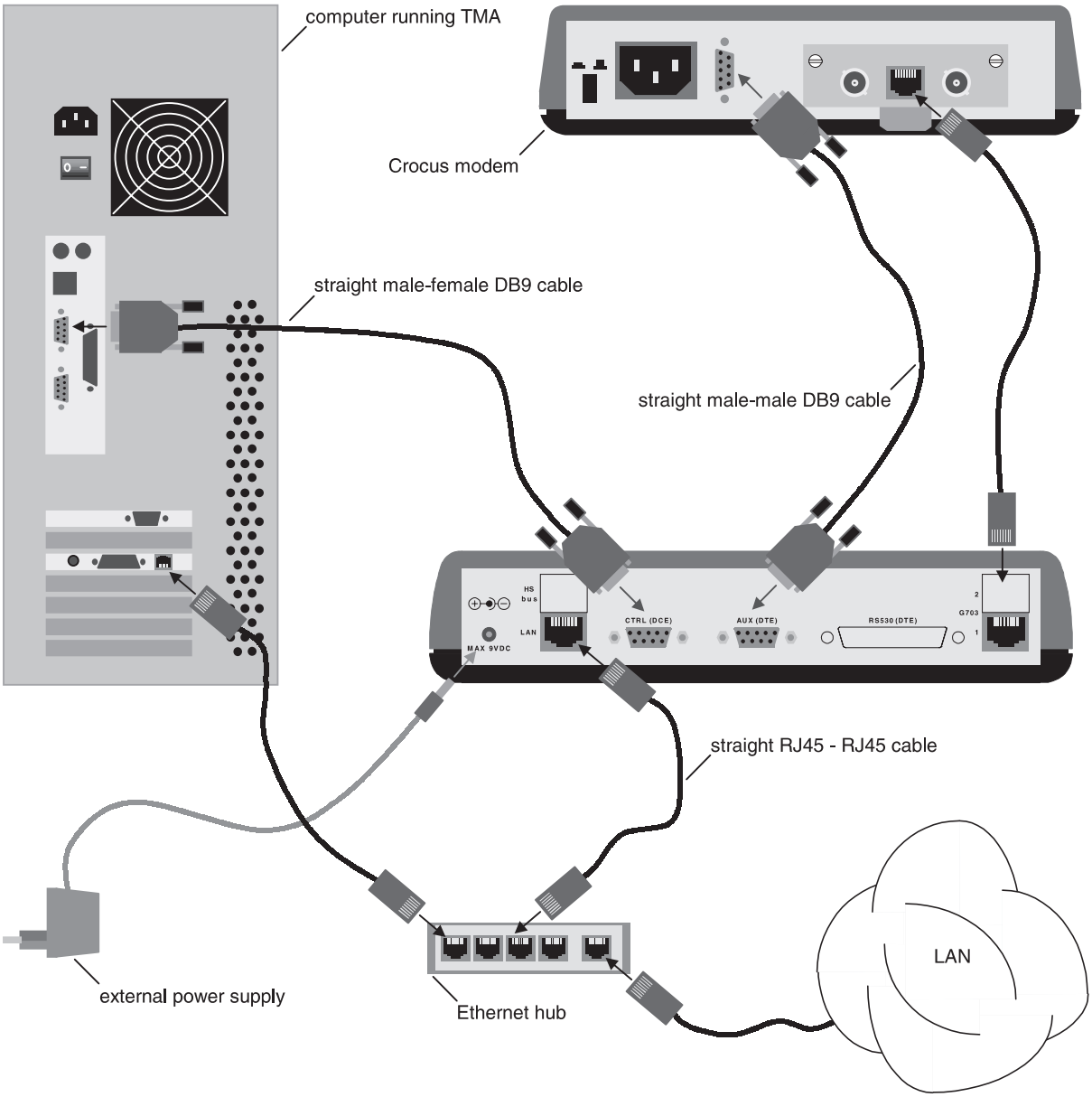
The following table gives an overview of the parts located at the back of the Telindus 1031 Router and reveals their function:

Part	Label	Function
1	9 VDC	This is the power input. Insert the plug of the external power supply in this socket.
2	LAN	This RJ45 Twisted Pair Interface (TPI) is the connection towards the IP LAN. Connect one side of an RJ45 to RJ45 cable (not included) to the LAN connector of the Telindus 1031 Router and the other side to a network outlet. If you want to connect the Telindus 1031 Router to … • a regular Ethernet network outlet, then use a crossed RJ45 cable. • an Ethernet hub, then use a straight RJ45 cable. Refer to 17.2 - LAN interface specifications on page 363 for the specifications of this connector.
3	CTRL (DCE)	This female 9-pins subD connector is the control connector. You can connect this connector to a COM port of your PC with a straight male-female DB9 cable[1]. This enables you to manage the Telindus 1031 Router locally, using TMA, CLI, ATWIN etc. You can also connect this connector to the control connector of another Telindus device with a crossed male-male DB9 cable. This enables you to manage this device with the Telindus 1031 Router (i.e. the Telindus 1031 Router as management concentrator). Refer to … • Refer to the Telindus 1030 Router Orchid function manual for more information on managing Telindus devices. • 17.3 - Control connector specifications on page 364 for the specifications of this connector.
4	AUX (DTE)	This female 9-pins subD connector is the auxiliary connector. You can connect this connector to the control connector of another Telindus device with a straight male-male DB9 cable[1]. This allows you to manage this device with the Telindus 1031 Router (i.e. the Telindus 1031 Router as management concentrator). Refer to … • Refer to the Telindus 1030 Router Orchid function manual for more information on managing Telindus devices. • 17.4 - Auxiliary connector specifications on page 365 for the specifications of this connector.
5	G703	This RJ45 connector is the serial G703 interface towards the WAN. Refer to 17.1 - G703 interface specifications on page 362 for the specifications of this connector.

1. Refer to the TAP catalogue for the layout and the sales codes of these cables.

2.5.3 Connecting the Telindus 1031 Router - an example

The following figure shows a typical Telindus 1031 Router set-up:



In this set-up …

- the external power supply is connected to the power input.
- the LAN connector is connected to an Ethernet hub using a straight RJ45 - RJ45 cable. In this way the Telindus 1031 Router is connected to your local network (LAN).
- the CTRL connector is connected to the COM port of a computer using a straight male - female DB9 cable. In this way you can, for example, manage the Telindus 1031 Router locally using TMA (CLI), CLI, ATWIN, etc.
- the AUX connector is connected to the control connector of a Crocus modem using a straight male - male DB9 cable. In this way the Telindus 1031 Router can manage the Crocus modem. Refer to the Telindus 1030 Router Orchid function manual for more information on managing Telindus devices.
- the G703 connector is connected to the G703 interface of a Crocus modem. In this way the Telindus 1031 Router is connected to the WAN. You can, for example, connect the Telindus 1031 Router to a

remote network over a leased line. Refer to 1.2 - Telindus 1031 Router applications on page 5 for some typical applications.

2.6 The front panel LED indicators

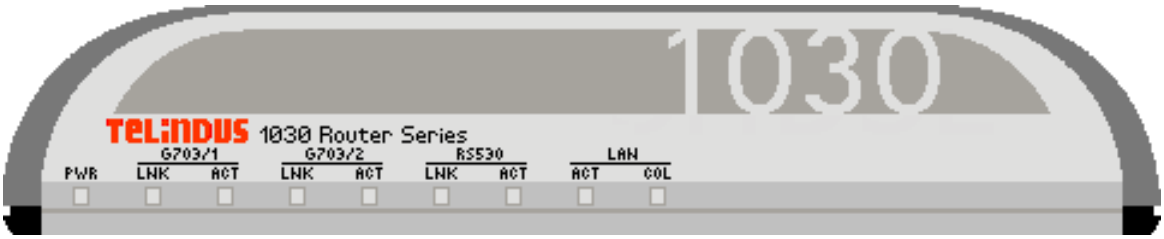
This section gives an overview of the front panel LEDs and what they indicate. The following gives an overview of this section:

- 2.6.1 - Introducing the front panel LEDs on page 25
- 2.6.2 - The power LED (PWR) on page 26
- 2.6.3 - The G703 link LED (G703 LNK) on page 26
- 2.6.4 - The G703 data LED (G703 ACT) on page 26
- 2.6.5 - The LAN LED (LAN ACT) on page 26
- 2.6.6 - The LAN collision LED (LAN COL) on page 27

2.6.1 Introducing the front panel LEDs

When all the connections are made and the Telindus 1031 Router is powered, the LEDs on the front panel reflect the actual status of the device.

The following figure shows the front panel LED indicators of the Telindus 1031 Router:



LED states

One front panel LED can reflect different status modes by the way it lights up. The front panel LEDs can light up as follows:

LED state	LED duty cycle	Description
continuously off	0 %	The LED never lights up.
continuously on	100 %	The LED lights up continuously.
blinking	50 %	The LED is as much lit as it is out.
flashing	20 %	The LED only lights up during 20% of the time.
mostly off	-	The LED occasionally lights up, without a fixed duty cycle.
mostly on	-	The LED occasionally goes out, without a fixed duty cycle.
monitoring	-	The LED lights up irregularly. For instance, it lights up on detection of a certain signal. I.e. it monitors this signal.

2.6.2 The power LED (PWR)

The power LED indicates the following:

LED status	Description
continuously off	No DC input power is available.
blinking	The self test, performed during the boot sequence, failed. In this condition, the ACT LEDs are continuously on.
continuously on	The Telindus 1031 Router is powered and the boot sequence has been completed successfully. In case the Telindus 1031 Router remains in boot mode, also the ACT LEDs are continuously on to indicate this special state. Refer to 16.1 - What is boot, loader and application software? on page 354 for more information on boot mode.

2.6.3 The G703 link LED (G703 LNK)

This LED reflects the status of the link on the G703 interface:

LED status	Description
continuously off	Loss Of Synchronisation (LOS), Loss of Frame Alignment (LFA) or Alarm Indication Signal (AIS, also called “all ones”) is received on the interface. LFA and AIS is only relevant in case of G.704 framing.
continuously on	Layer 1 (G.704 framing) is up.

2.6.4 The G703 data LED (G703 ACT)

This LED reflects the status of the user data on the G703 interface:

LED status	Description
continuously off	Layer 2 is down.
monitoring	Layer 2 is up and user data is present (both transmit and receive data).
continuously on	Layer 2 is up, but no user data is present.

If the G703 interface has multiple logical interfaces (channelised E1), it indicates only the status for the first logical interface on this physical interface.

2.6.5 The LAN LED (LAN ACT)

This LED reflects the status of the link and monitors the user data on the LAN interface:

LED status	Description
continuously off	Nothing is connected to the LAN interface.
monitoring	The Ethernet link is up and there is network activity on the LAN.
continuously on	The Ethernet link is up, but there is no network activity on the LAN.

2.6.6 The LAN collision LED (LAN COL)

This LED lights up each time there is an Ethernet frame collision on the LAN.

3 DIP switches of the Telindus 1031 Router

This chapter locates the DIP switches on the Telindus 1031 Router motherboard. It gives an overview of their function and it explains how to change their settings.

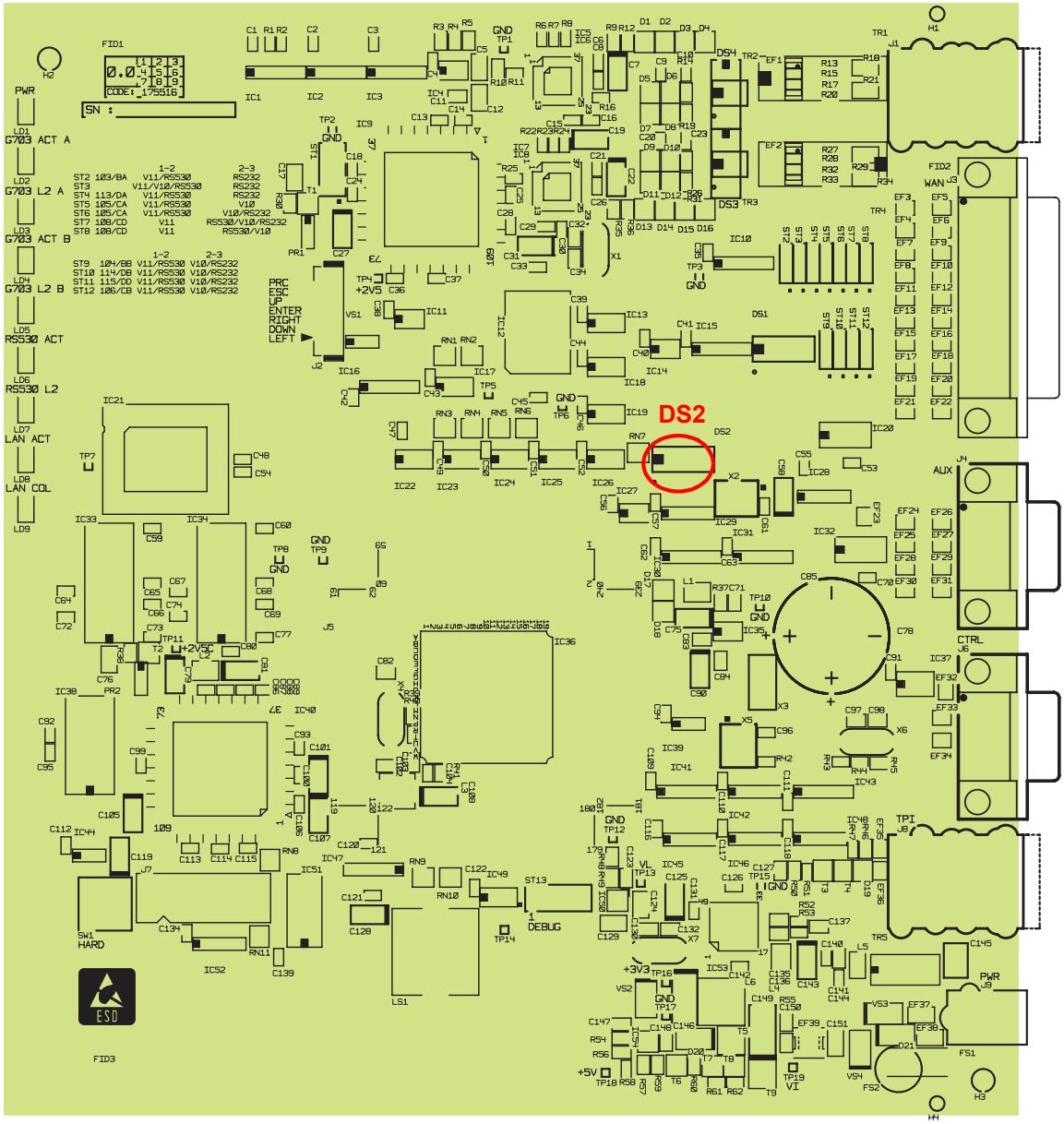
The following gives an overview of this chapter:

- 3.1 - The Telindus 1031 Router motherboard on page 30
- 3.2 - DIP switches of the Telindus 1031 Router on page 31
- 3.3 - Opening and closing the housing on page 32

Default settings are printed in **bold**.

3.1 The Telindus 1031 Router motherboard

The figure below shows the position of the DIP switches on the Telindus 1031 Router motherboard:



3.2 DIP switches of the Telindus 1031 Router

The following table gives an overview of the DIP switches on DIP switch bank DS2:

DIP switch name	DS2 no.	Setting	Function
loader mode	1	**on**	Normal operation.
		off	Start up in loader mode.
load default configuration	2	**on**	Normal operation.
		off	Load default configuration.

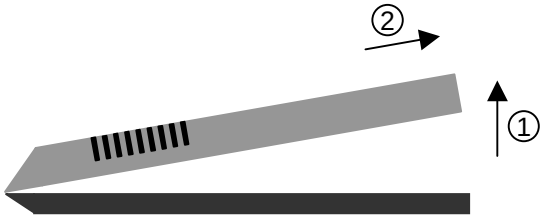
Refer to 3.3 - Opening and closing the housing on page 32 to find out how to open the housing in order to change the DIP switch settings.

3.3 Opening and closing the housing

When you want to change the DIP switch settings, you have to open and close the housing of the Telindus 1031 Router. This section explains how to do so.

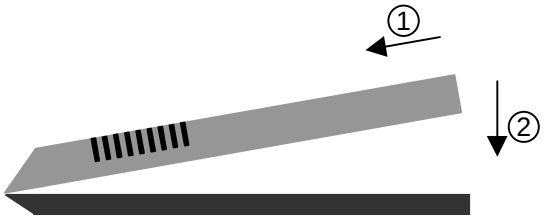
Opening the housing

To open the housing of the Telindus 1031 Router, proceed as follows:

Step	Action
1	Disconnect the external power supply.
2	Unscrew the two screws located at the back of the housing.
3	Remove the cover as follows: 1. Carefully lift the back of the cover a few centimetres. 2. Gently pull the cover backwards from under the nose of the housing. 

Closing the housing

To close the housing of the Telindus 1031 Router, proceed as follows:

Step	Action
1	Replace the cover as follows: 1. Gently push the cover under the nose of the housing. 2. Lower the back of the cover. 3. Push on the back of the cover, clicking cover and bottom together. 
2	Fasten the two screws located at the back of the housing.
3	Reconnect the external power supply.

4 Managing the Telindus 1031 Router

Once you installed the Telindus 1031 Router, you can proceed with the configuration of the Telindus 1031 Router. You can do this using any of the management tools introduced in 1.4 - Management tools on page 10.

This chapter briefly highlights one of those management tools: the Telindus Maintenance Application (TMA). It introduces TMA and describes how to start a session on the Telindus 1031 Router. It also introduces the terminology concerning the management of a Telindus device. Furthermore, it explains why and how to add an object to the containment tree.

The following gives an overview of this chapter:

- 4.1 - Managing the Telindus 1031 Router with TMA on page 34
- 4.2 - Introducing the management terminology on page 40
- 4.3 - The objects in the Telindus 1031 Router containment tree on page 44
- 4.4 - Adding an object to the containment tree on page 45
- 4.5 - Telindus 1031 Router attribute overview on page 50

4.1 Managing the Telindus 1031 Router with TMA

First, this section introduces TMA. Then it describes how to start a session on the Telindus 1031 Router. The following gives an overview of this section:

- 4.1.1 - What is TMA? on page 35
- 4.1.2 - How to connect TMA? on page 35
- 4.1.3 - Connecting through the control connector on page 36
- 4.1.4 - Connecting over an IP network on page 38

4.1.1 What is TMA?

TMA is the acronym for Telindus Maintenance Application. TMA is a free Windows software package that enables you to maintain the Telindus 1031 Router, i.e. to access its configuration attributes and look at status, performance and alarm information using a user friendly graphical user interface.

TMA is an excellent tool for complete management of the Telindus access devices. When using TMA in combination with a network management system such as HP OpenView, complete networks can be managed from one central site.

Consult the TMA manual how to install TMA and to get acquainted with the user interface.

You will need a new version of the model file distribution if changes have been made to the attributes of the Telindus 1031 Router. The most recent model files and TMA engine can always be downloaded from the Telindus web site at http://www.telindusproducts.com/TMA.

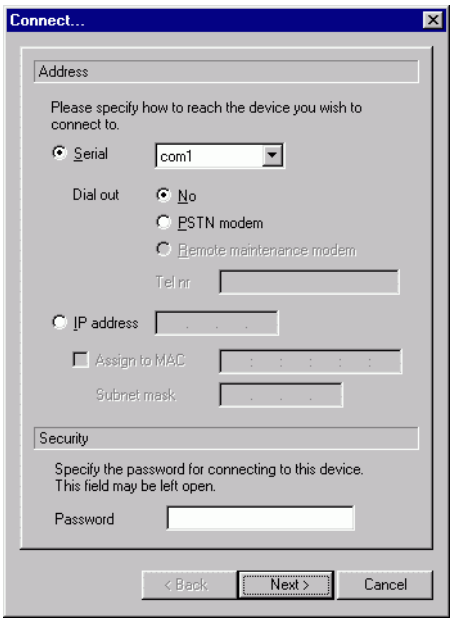
4.1.2 How to connect TMA?

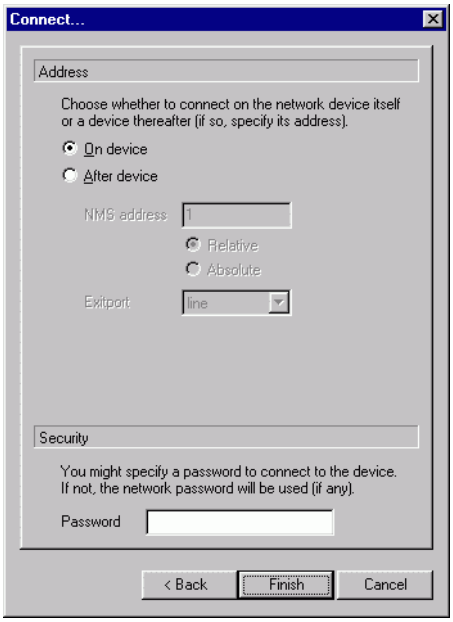
There are two ways to establish a connection between the computer running TMA and the Telindus 1031 Router:

- through a serial connection, i.e. through the control connector of the Telindus 1031 Router. Refer to 4.1.3 - Connecting through the control connector on page 36.
- through an IP connection, i.e. through the LAN connector of the Telindus 1031 Router. Refer to 4.1.4 - Connecting over an IP network on page 38.

4.1.3 Connecting through the control connector

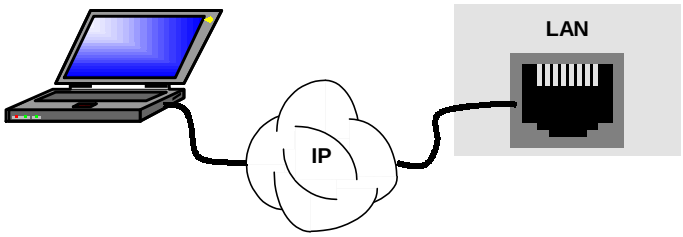
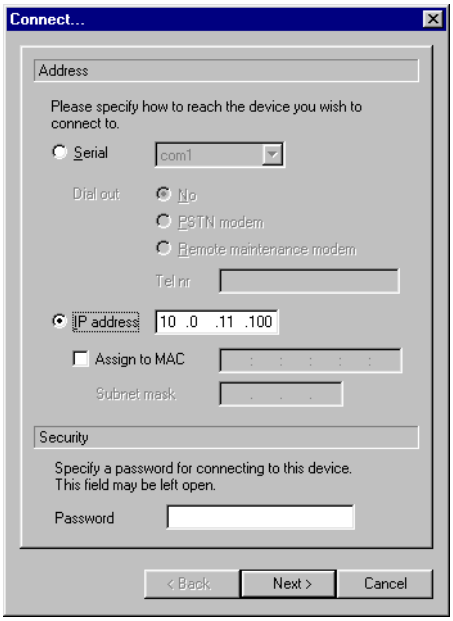
To established a connection between TMA and the Telindus 1031 Router through the control connector, proceed as follows:

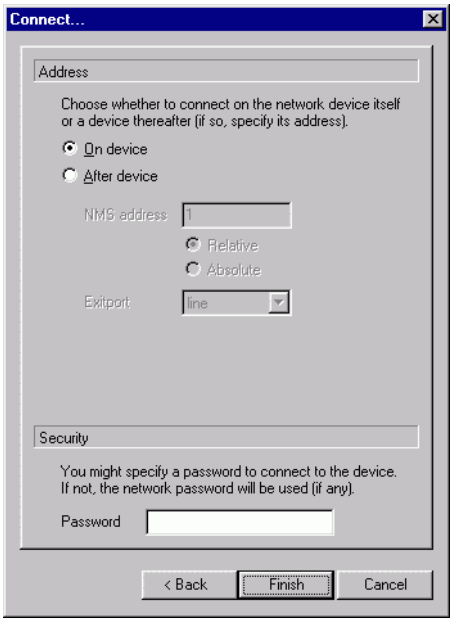
Step	Action
1	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the control connector of the Telindus 1031 Router.
2	Start TMA.
3	In the TMA window, either … • select from the menu bar: *Connect* → *Device…* • or press the short-cut key: Ctrl+N • or click on the *Connect to device* button: The *Connect…* (to a device) window is displayed as in the following figure: 
4	In the *Connect…* (to a device) window, specify the following: • Select the option *Serial* and specify the COM port of your computer to which the Telindus 1031 Router is connected. • If previously a password has been configured in the Telindus 1031 Router then also fill in the password field.
5	Click on the *Next* > button. ⇒The second *Connect…* window is displayed.

Step	Action
6	In the *Connect…* (select a device) window, specify the following: • Select the option *On device*. • If previously a password has been configured in the Telindus 1031 Router then also fill in the password field. 
7	Click on the *Finish* button.
8	After a couple of seconds, the attributes of the Telindus 1031 Router appear in the TMA window.

4.1.4 Connecting over an IP network

To established a connection between TMA and the Telindus 1031 Router over an IP network, proceed as follows:

Step	Action
1	Connect the IP network to … • the network port of your PC, • the LAN connector of the Telindus 1031 Router. 
2	Start TMA.
3	In the TMA window, either … • select from the menu bar: *Connect* → *Device…* • or press the short-cut key: Ctrl+N • or press on the *Connect to device* button: The *Connect…* (to a device) window is being displayed as in the following figure: 
4	In the *Connect…* (to a device) window, specify the following: • Select the option *IP address* and enter the IP address of the Telindus 1031 Router. • If a password has previously been configured in the Telindus 1031 Router then also fill in the password field. Before you are able to establish a connection over an IP network, you have to configure an IP address and a default gateway in the Telindus 1031 Router. You can do this by first connecting TMA to the Telindus 1031 Router through the control connector, and then configuring an IP address and a default gateway. Refer to the 5.2 - Configuring IP addresses on page 55.
5	Click on the *Next* > button. ⇒The second *Connect…* window is displayed.

Step	Action
6	In the *Connect…* (select a device) window, select the option *On device*. 
7	Click on the *Finish* button.
8	After a couple of seconds, the attributes of the Telindus 1031 Router appear in the TMA window.

4.2 Introducing the management terminology

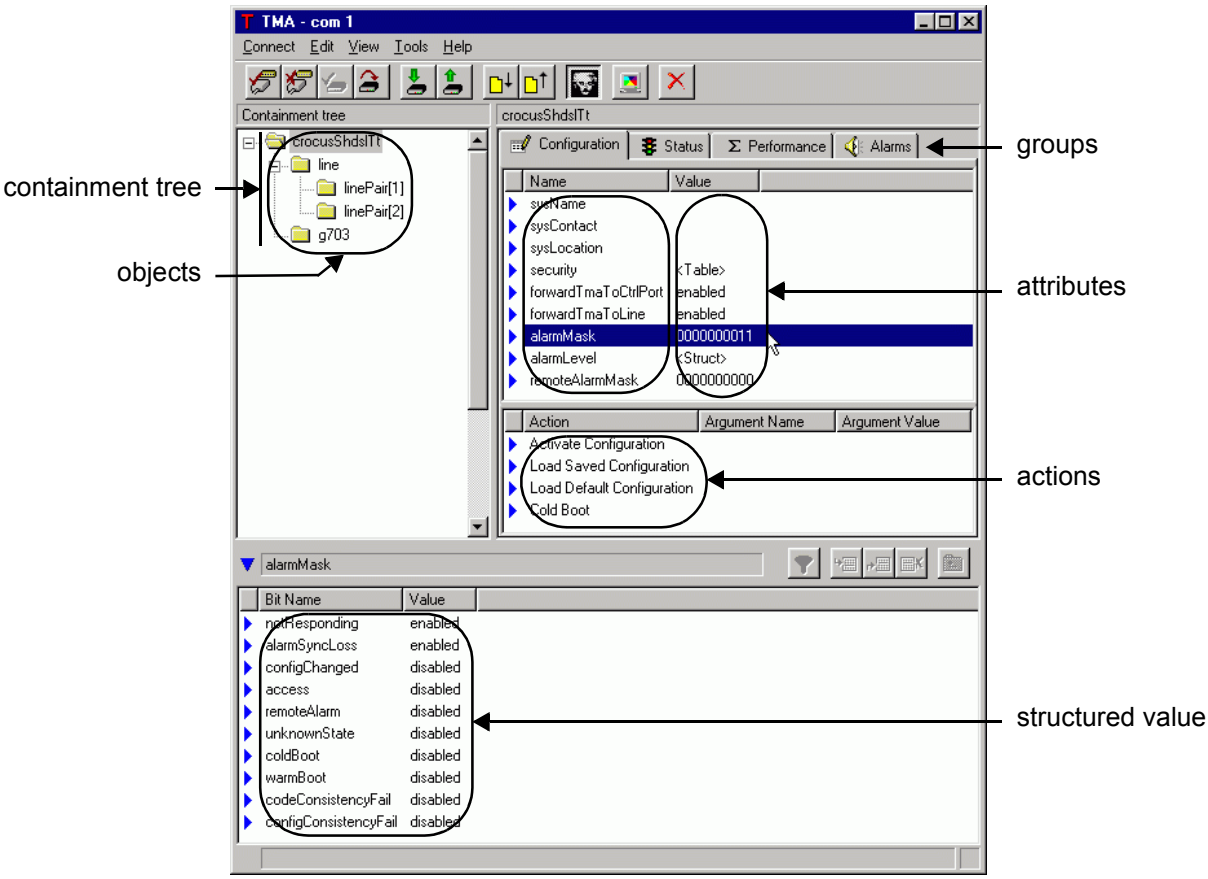
This section briefly introduces the terminology concerning the management of a Telindus device. It explains terms such as containment tree, group, object, attribute, value and action.

The following gives an overview of this section:

- 4.2.1 - Graphical representation of the containment tree on page 41
- 4.2.2 - Containment tree terminology on page 42

4.2.1 Graphical representation of the containment tree

The most comprehensible graphical representation of the containment tree is given in TMA. The following figure depicts the TMA window displaying a containment tree:



Refer to 4.2.2 - Containment tree terminology on page 42 for an explanation of the terms associated with the containment tree.

4.2.2 Containment tree terminology

Refer to 4.2.1 - Graphical representation of the containment tree on page 41 for a figure of a containment tree.

The following table explains the terminology associated with the containment tree:

Term	Description
containment tree	The containment tree represents the hierarchical structure of the Telindus 1031 Router. It is composed of a number of objects that are ordered in a tree. This tree resembles a Windows directory structure: • it is also a levelled structure, with nodes which can be expanded or reduced. • the containment tree objects can be compared with file folders. • the objects contain attributes like file folders contain files.
object	An object represents a physical interface, an application or a combination of both. Each object has its own set of attributes.
parent and child object	Some objects are not present in the containment tree by default. If you want to use the features associated with such an object, then you have to add the object first. You always add an object under another object. The object you add is called the child object. The object under which you add this child object is called the parent object.
index name	Of some objects more than one object is present in the containment tree. The different objects are distinguished from one another by adding an index. E.g. linePair[1] and linePair[2], where 1 and 2 are the indexes. Also child objects are given an index (by the user when adding the object). An index name is also often referred to as *index*, *instance value* or *instance name*.
attribute	An attribute is a parameter related to a certain object. It has a certain value.
value	An attribute has a certain value which is … • changeable in case of a configuration attribute (provided you have write access). • read only in case of a status, performance and alarm attribute.
structured value	Some attribute values contain underlying values: a structured value. These values are displayed in the structured value window. If an attribute contains structured values, then a bit string, <Table> or <Struct> is displayed after the attribute. A structured value is also often referred to as just *structure*.

Term	Description
element	An element is an attribute within a structured value. In other words, they could be considered as “sub-attributes”.
group	Groups assemble a set of attributes related by functionality. There are four groups in TMA, which correspond with the four tabs in the attribute window: • configuration, • status, • performance, • alarms.
action	A group in combination with an object may have actions assigned to them. These actions are displayed in the action window.

4.3 The objects in the Telindus 1031 Router containment tree

The following table lists the different objects of the Telindus 1031 Router containment tree:

> telindus1031
>> lanInterface
>> g703[1]
>>> channel[g703_1]
>>>> ppp
>>>> frameRelay
>>>> atm
>>>> hdlc
>> router
>>> tunnels
>>> routingFilter[ ][1]
>>> priorityPolicy[ ][1]
>>> trafficPolicy[ ][1]
>>> defaultNat
>> bridge
>>> bridgeGroup
>>> accessList[ ][1]
>> snmp
>> management
>>> loopBack
>> proxy[1]
>> fileSystem
>> operatingSystem

1. Not present by default. Has to be added (refer to 4.4 - Adding an object to the containment tree on page 45). The index name is user defined.

4.4 Adding an object to the containment tree

This section explains why and how you can add an object to the containment tree. It then explains why and how to refer to this object.

The following gives an overview of this section:

- 4.4.1 - Why add an object to the containment tree? on page 46
- 4.4.2 - How to add an object to the containment tree? on page 47
- 4.4.3 - Referring to an added object on page 49

4.4.1 Why add an object to the containment tree?

Why can you add an object to the containment tree?

Some objects are not present in the containment tree by default but you can add them yourself because …

- in this way the containment tree remains clear and surveyable,
- you possibly do not need the functions associated with such an object,
- you possibly need several of these objects so you can add as many objects as you like.

When do you have to add an object to the containment tree?

If you want to use the features associated with such an object, then you have to add the object first.

Which objects can be added to the containment tree?

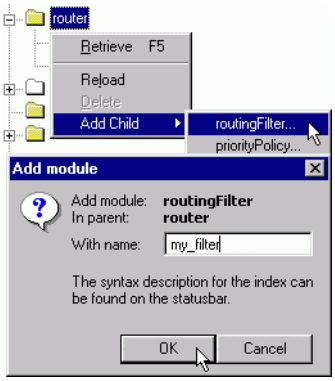
Section 4.3 - The objects in the Telindus 1031 Router containment tree on page 44 gives you an overview of all the objects in the containment tree. It also tells you which objects have to be added before you can use them.

4.4.2 How to add an object to the containment tree?

The section shows you, for each management tool, how to add an object to the containment tree. The following section, 4.4.3 - Referring to an added object on page 49, shows you how you can “refer” to this added object somewhere else in the containment tree.

Adding an object in TMA

Step	Action
1	Right click on the parent object (e.g. router). ⇒A pop-up menu appears.
2	In the pop-up menu, select *Add Child…* and select the child object you want to add (e.g. routingFilter). ⇒A pop-up window appears.
3	In the pop-up window, type the instance value (i.e. the index name) for the child object (e.g. my_filter) and click on *OK*. ⇒The new child object is created (e.g. routingFilter[my_filter]).



Adding an object in (TMA) CLI

Step	Action
1	Enter the parent object (e.g. `select router`).
2	Type the following command: `set {select childObjectName[instanceValue]{}}` where `instanceValue` is a string of your choice. (e.g. `set {select routingFilter[my_filter]{}}`) ⇒The new child object is created.

Adding an object in ATWIN

Step	Action
1	Enter the parent object (e.g. go to the router object and press the enter key). ⇒The ATWIN window shows the sub-objects and attributes of the parent object.
2	Go to the line displaying the string `<CREATE INSTANCE>` and the name of the object you want to add (e.g. `routingFilter <CREATE INSTANCE>`) and press the enter key. ⇒A new window appears, displaying the string `Give the instanceValue`.
3	Press the enter key and type the instance value (i.e. the index name) for the child object (e.g. my_filter) and press the enter key again. ⇒The new child object is created (e.g. `>.routingFilter [name:my_filter])`.

Adding an object in the Web Interface

Step	Action
1	Enter the parent object (e.g. select the router object and double-click it or click on *Open*). ⇒The Web Interface window shows the sub-objects and attributes of the parent object.
2	Select the line displaying the string `<CREATE INSTANCE>` and the name of the object you want to add (e.g. `routingFilter <CREATE INSTANCE>`) and double-click it or click on *Open*. ⇒A new window appears, displaying the string `Give the instanceValue`.
3	Type the instance value (i.e. the index name) for the child object (e.g. my_filter) and click on *exit*. ⇒The new child object is created (e.g. `>.routingFilter [name:my_filter]`).

4.4.3 Referring to an added object

What is referring to an added object?

If at a certain place in the containment tree you want to apply the function associated with an object you added, then you have to refer to this object.

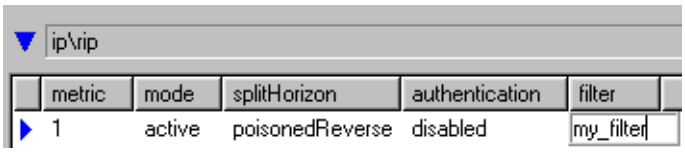
How to refer to an added object?

Some attributes allow you to enter the instance value (i.e. the index name you assigned to the object) of an added object. By doing so, the function associated with this object is applied there.

Example

Suppose you create a routingFilter object with the instance value my_filter. The containment tree then looks as follows:

Now, you want to use this filter on the LAN interface. In that case, in the ip/rip structure in the lanInterface object, enter the instance value of the routingFilter object under the element “filter”. This looks as follows:



4.5 Telindus 1031 Router attribute overview

The reference part of this manual explains all the attributes of the Telindus 1031 Router. One chapter describes one group of attributes:

- chapter 10 - Configuration attributes on page 171,
- chapter 11 - Status attributes on page 245,
- chapter 12 - Performance attributes on page 299,
- chapter 13 - Alarm attributes on page 327.

5 Basic configuration

This chapter shows you how to configure the very basics of the Telindus 1031 Router. This will allow you to access the Telindus 1031 Router over an IP connection with, for example, TMA. First this chapter explains how DIP switch configuration tables and TMA attribute strings should be interpreted.

The following gives an overview of this chapter:

- 5.1 - Reading DIP switch tables and TMA attribute strings on page 52
- 5.2 - Configuring IP addresses on page 55
- 5.3 - Configuring the G703 interface on page 61
- 5.4 - Configuring passwords on page 62
- 5.5 - Configuring the major features of the Telindus 1031 Router on page 65
- 5.6 - Executing configuration actions on page 66

Refer to the Reference manual on page 169 for a complete overview of the attributes of the Telindus 1031 Router.

5.1 Reading DIP switch tables and TMA attribute strings

As this chapter explains the basic configuration of the Telindus 1031 Router, it contains some DIP switch tables and a lot of TMA attribute strings. To enable you to read this information in a correct manner, this section explains the structure of such tables and strings.

The following gives an overview of this section:

- 5.1.1 - Reading a DIP switch table on page 53
- 5.1.2 - Reading a TMA attribute string on page 54

5.1.1 Reading a DIP switch table

A DIP switch configuration table has the following layout:

DIP switch name	DS1 no.	Setting	Function
	1	**on**	
		off	

1 **2** **3** **4** **5**

The following table explains the DIP switch configuration table layout:

Number	This position displays …
1	the DIP switch icon.
2	the DIP switch name.
3	the DIP switch position on the DIP switch bank. The abbreviations mean the following: DS1 no. 1: DIP switch bank number 1, switch position number 1
4	the possible settings of the DIP switch: on and off. The default setting is printed in bold.
5	the function associated with the corresponding DIP switch setting.

5.1.2 Reading a TMA attribute string

A TMA attribute string has the following layout:

1 **2** **3**

The following table explains the TMA attribute string layout:

Number	This position displays …
1	the TMA attribute icon. It indicates that the string which follows is a TMA attribute string. Refer to Graphical conventions on page vi for more information.
2	the attribute name and its position in the containment tree.
3	the default value of a configuration attribute.

5.2 Configuring IP addresses

The first thing you have to configure are the IP addresses of the Telindus 1031 Router. First this section lists which mechanisms there are to obtain an IP address automatically. Then it shows you, for each interface, where you can find the IP related parameters. Finally this section explains these IP related parameters.

The following gives an overview of this section:

- 5.2.1 - Automatically obtaining an IP address on page 56
- 5.2.2 - Where to find the IP related parameters on page 57
- 5.2.3 - Explaining the ip structure on page 58

5.2.1 Automatically obtaining an IP address

Obtaining an IP address on the LAN interface

The Telindus 1031 Router supports the BootP protocol to automatically obtain an IP address on its LAN interface.

Refer to 15 - Auto installing the Telindus 1031 Router on page 341 for more information on auto-install.

Obtaining an IP address on the WAN interface

Currently the Telindus 1031 Router does not support any protocols to automatically obtain an IP address on its WAN interface. However, if you do not configure an IP address on the WAN interface, then the IP address of the LAN interface is used. In other words, the LAN interface shares its IP address with the WAN interface. This is called unnumbered mode.

An IP address that was obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.

5.2.2 Where to find the IP related parameters

Each interface[1] has a structured configuration attribute named “ip”. In this structure you can configure the IP related parameters for that interface.

The following table shows where you can find the ip structure for the different interfaces:

<table>
<tr><th>For the …</th><th>you can find the ip structure in …</th></tr>
<tr><td>LAN interface,</td><td>the lanInterface object: telindus1031/lanInterface/ip.

Important remark

If you set the configuration attribute telindus1031/lanInterface/mode to bridging, then the settings of the configuration attribute telindus1031/lanInterface/ip are ignored. As a result, if you want to manage the Telindus 1031 Router via IP, you have to configure an IP address in the bridgeGroup object instead: telindus1031/bridge/bridgeGroup/ip.</td></tr>
<tr><td>WAN interface,</td><td>each WAN encapsulation object:

<table>
<tr><td>frameRelay</td><td>You can find the ip structure on two levels:
• in the frameRelay object: telindus1031/g703[ ]/channel[ ]/frameRelay/ip.
• in the dlciTable attribute: the ip element in telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable.

Section 6.3.2 - Configuring IP addresses on the Frame Relay WAN on page 80 explains why.</td></tr>
<tr><td>ppp</td><td>You can find the ip structure in the ppp object: telindus1031/g703[ ]/channel[ ]/ppp/ip.</td></tr>
<tr><td>atm</td><td>You can find the ip structure in the pvcTable attribute: the ip element in telindus1031/g703[ ]/channel[ ]/atm/pvcTable.</td></tr>
</table>
</td></tr>
<tr><td>tunnels,</td><td>the l2tpTunnels attribute: the ip element in telindus1031/router/tunnels/l2tpTunnels.</td></tr>
<tr><td>bridge,</td><td>the bridgeGroup object: telindus1031/bridge/bridgeGroup/ip.</td></tr>
</table>

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

1. The interface can be a physical interface (such as the LAN interface), but can also be a DLCI, a PVC, a tunnel, etc.

5.2.3 Explaining the ip structure

Because the ip structure occurs in several objects, it is described here once and referenced where necessary. Refer to 5.2.2 - Where to find the IP related parameters on page 57 for the location of the ip structure.

This section lists all the elements that can be present in the ip structure. However, depending on the interface, it is possible that not all of these elements are present.

The ip structure contains the following elements:

Element	Description
address	Use this element to assign an IP address to the interface. The address should belong to the subnet the interface is connected to. Default:0.0.0.0 Range: up to 255.255.255.255
netMask	Use this element to assign an IP subnet mask to the interface. The subnet mask defines the number of IP devices that may be present on the corresponding IP segment. Default:255.255.255.0 Range: up to 255.255.255.255
secondaryIp	This element is only present for the LAN interface. Use this element to create additional virtual networks on the same Ethernet interface. Default:<empty> Range: table, see below The secondaryIp table contains the elements address and netMask. See above for an explanation of these elements.
remote	This element is only present for a Frame Relay DLCI, a PPP link, an ATM PVC and an L2TP tunnel. Use this element to assign an IP address to the remote end of the Frame Relay DLCI, PPP link, ATM PVC or L2TP tunnel. Default:0.0.0.0 Range: up to 255.255.255.255 If supported by the network, the Reverse ARP protocol can obtain the remote IP address automatically. In that case, the remote IP address is not displayed in the configuration window, but can be found in the status window.
rip	Use this element to configure the RIP related parameters of the interface. Default:- Range: structure, see below Refer to 7.3.3 - Explaining the rip structure on page 110 for a detailed description of the rip structure.

Element	Description
trafficPolicy	This element is not present in the telindus1031/g703[ ]/channel[ ]/frameRelay/ip structure. You have to specify a traffic policy per DLCI. Use this element to apply a traffic policy on the routed data on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the traffic policy you want to use. You can create the traffic policy itself by adding a trafficPolicy object under the router object and by configuring the attributes in this object. **Example** If you created a trafficPolicy object with index name my_traffic_policy (i.e. trafficPolicy[my_traffic_policy]) and you want to apply this traffic policy here, then enter the index name as value for the trafficPolicy element. Refer to … • 7.6 - Configuring traffic and priority policy on the router on page 130 for more information on policies. • 4.4 - Adding an object to the containment tree on page 45 for more information on adding objects. On the LAN interface, you can not apply a traffic policy with the purpose of queueing. On this interface, the traffic policy is intended to serve as extended access list. Refer to 7.7 - Configuring an extended access list on page 138.
directedBroadcasts	Use this element to enable (forward) or disable (discard) directed broadcasts. Default:enabled Range: enabled / disabled **What is a directed broadcast?** A directed broadcast is an IP packet destined for a complete (sub-)network. For example, a packet destined for all devices on subnetwork 192.168.48.0 with subnet mask 255.255.255.0 has destination address 192.168.48.255. I.e. all ones in the subnet area of the IP address.
icmpRedirects	Use this element to enable or disable the transmission of ICMP messages. Default:enabled Range: enabled / disabled **What is an ICMP redirect?** If icmpRedirects is enabled and if the Telindus 1031 Router receives an IP packet on the interface for which … • the next hop gateway is on the same interface, • the next hop address is in the same subnet as the source, … then it sends an ICMP message to the originator of the packet to inform him that a better (shorter) route exists.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>igmp</td><td>
Use this element to configure the multicasting IGMP protocol.
Default:disabled
Range: enumerated, see below

The igmp element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>Multicasts are not forwarded on this interface.</td></tr>
<tr><td>proxy</td><td>This is an upstream interface. It always serves as a client for the upstream router.

Multicasts are always forwarded on this interface.</td></tr>
<tr><td>router</td><td>This is a downstream interface. It serves as an IGMP querier or non-querier depending on the IP address.

Multicasts are forwarded on this interface if they are present in the upstream-interface multicast-member list.</td></tr>
</table>

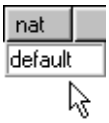
Refer to What is IGMP? and IGMP topology on page 277 for more information on IGMP.
</td></tr>
<tr><td>helperAddresses</td><td>
Use this element to enable broadcast forwarding.
Default:<empty>
Range: table, see below

Limited IP broadcasts (address 255.255.255.255) and (sub-)network broadcasts for a directly connected network are normally not forwarded by the Telindus 1031 Router. However, client / server applications often use these broadcasts during start-up to discover the server on the network. If the server is on a remote LAN, then the detection may fail.

Therefore, if you configure a helper IP address, the received broadcasts address is replaced by this helper IP address and the packets are re-routed using the destination address. Multiple helper IP addresses can be configured.

The Telindus 1031 Router only substitutes addresses for the protocols which are selected in the helperProtocols attribute. Refer to telindus1031/router/helperProtocols on page 208.
</td></tr>
<tr><td>nat</td><td>
Use this element to enable Network Address Translation on the interface.
Default:<empty>
Range: 0 … 24 characters

Do this by entering the string “default“ as nat element value. By doing so, the NAT settings are applied as defined in the defaultNat object under the router object. In future releases, it will also be possible to refer to user defined NAT object (analogous to the routing filter, traffic policy, etc.).



Refer to …
• 7.4 - Configuring address translation on page 116 for more information on NAT.
• 10.5.2 - Default NAT configuration attributes on page 215 for a detailed description of the NAT configuration attributes.
</td></tr>
</table>

5.3 Configuring the G703 interface

This sections lists the most essential attributes to configure the G703 interface:

- Use the coding attribute to set the G703 interface encoding mode. Refer to telindus1031/g703[ ]/coding on page 182.
- Use the framing attribute to select between unframed or framed mode. Refer to telindus1031/g703[ ]/framing on page 182.
- Use the clocking attribute to select a clocking mode. Refer to telindus1031/g703[ ]/clocking on page 182.
- Use the crc4Insertion attribute to determine whether the CRC-4 (Cyclic Redundancy Check) is recalculated before sending it to the interface. The CRC is used to check the data integrity on the G.703 connection. Refer to telindus1031/g703[ ]/crc4Insertion on page 183.
- If you have set the framing attribute to framed, then use the timeSlots attribute to enable or disable the individual 64 kbps time slots in the framed data stream. Refer to telindus1031/g703[ ]/channel[ ]/timeSlots on page 184.

Important remark

You can only use ATM encapsulation on the G703 interface when you selected framed mode, not when you selected unframed mode (refer to telindus1031/g703[ ]/framing on page 182).

5.4 Configuring passwords

This section shows you how to create a (list of) password(s) with associated access level in the security table. It also explains how to correct the security table in case of error or in case you forgot your password. Furthermore, this section shows you how to enter the passwords in the different management tools.

The following gives an overview of this section:

- 5.4.1 - Creating passwords in the security table on page 63
- 5.4.2 - Correcting the security table on page 63
- 5.4.3 - Entering passwords in the different management tools on page 64

5.4.1 Creating passwords in the security table

In order to avoid unauthorised access to the Telindus 1031 Router and the network you can create a list of passwords with associated access levels in the security table. Do this using the security attribute. Refer to telindus1031/security on page 175.

5.4.2 Correcting the security table

If you forgot your password or you forgot to create one with write and security access, then you can set the *Load Default Configuration* DIP switch. As a result, the Telindus 1031 Router reboots in its default configuration. You can then retrieve the erroneous configuration and correct it.

To correct the security table, proceed as follows:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 32.
2	Set DIP switch bank DS2 position 2 to *off*. Refer to 3.1 - The Telindus 1031 Router motherboard on page 30 to locate this DIP switch bank.
3	Replace the cover without fastening the screws and reconnect the power supply. ⇒The Telindus 1031 Router reboots and loads the default configuration.
4	Retrieve the erroneous configuration: **Step** / **Action** 1 — Open a TMA session on the Telindus 1031 Router. Refer to 4.1 - Managing the Telindus 1031 Router with TMA on page 34. 2 — Execute the Load Saved Configuration action. 3 — Change the password and/or access rights in the security table. 4 — Execute the Activate Configuration action.
5	Again, disconnect the power supply and open the housing.
6	Reset DIP switch bank DS2 position 2 to *on*.
7	Properly replace the cover as described in 3.3 - Opening and closing the housing on page 32 and reconnect the power supply.

5.4.3 Entering passwords in the different management tools

Now that you created a (list of) password(s) in the Telindus 1031 Router, you have to enter these passwords every time you want to access the Telindus 1031 Router with one of the management tools.

The following table explains how to enter passwords in the different management tools:

Management tool	How to enter the password?
TMA	Enter the password in the *Connect…* window.
TMA CLI and TMA for HP OpenView	Use the application *TmaUserConf.exe* to create a TMA user and assign a password to this user. The password should correspond with a password configured in the device. Refer to the manual of TMA CLI or TMA for HP OpenView for more information.
CLI	You are prompted to enter the password when the session starts.
ATWIN	You are prompted to enter the password when the CLI session starts. Then you can start an ATWIN session.
Web Interface	You are prompted to enter the password when the session starts.
SNMP	Define the password as community string. If no passwords are defined, then you can use any string as community string.
TML	Enter the password after the destination file name. Separate password and file name by a '?'. Example: `tml -fsourcefile@destinationfile?pwd`
TFTP	Enter the password after the destination file name. Separate password and file name by a '?'. Example: `put sourcefile destinationfile?pwd`

5.5 Configuring the major features of the Telindus 1031 Router

The following list shows you where you can find an introduction to and a basic configuration of the most important features of the Telindus 1031 Router:

- 6.1 - Selecting a WAN encapsulation protocol on page 72
- 6.3 - Configuring Frame Relay encapsulation on page 77
- 6.2 - Configuring PPP encapsulation on page 73
- 6.4 - Configuring ATM encapsulation on page 86
- 7.2 - Configuring static routes on page 100
- 7.3 - Configuring the Routing Information Protocol on page 107
- 7.4 - Configuring address translation on page 116
- 7.5 - Configuring L2TP tunnelling on page 127
- 7.6 - Configuring traffic and priority policy on the router on page 130
- 7.7 - Configuring an extended access list on page 138
- 8.9 - Configuring bridging on page 149
- 8.10 - Configuring traffic and priority policy on the bridge on page 154
- Refer to the Telindus 1030 Router Orchid function manual for more information on the proxy function.

5.6 Executing configuration actions

This section shows you how to execute actions on the configuration. The following gives an overview of this section:

- 5.6.1 - What are the different configuration types? on page 67
- 5.6.2 - Activating the configuration on page 68
- 5.6.3 - Loading the saved configuration on page 68
- 5.6.4 - Loading the default configuration using the action on page 68
- 5.6.5 - Loading the default configuration using the DIP switch on page 69

5.6.1 What are the different configuration types?

This section explains the different configuration types that are present in the Telindus 1031 Router.

Which are the configuration types?

Three types of configuration are present in the Telindus 1031 Router:

- the non-active configuration
- the active configuration
- the default configuration.

Explaining the configuration types

When you configure the Telindus 1031 Router, the following happens:

Phase	Action	Result
1	Connect the computer running the management tool to the Telindus 1031 Router.	The non-active configuration is displayed on the screen.
2	Modify the non-active configuration.	The modifications have no immediate influence on the active configuration currently used by the Telindus 1031 Router.
3	Complete the modifications on the non-active configuration.	The non-active configuration has to be activated.
4	Execute the Activate Configuration action.	The non-active configuration becomes the active configuration.

What are the configuration actions?

You can execute the following actions on the configuration:

- activate configuration,
- load saved configuration,
- load default configuration.

5.6.2 Activating the configuration

telindus1031/Activate Configuration

If you execute this action, the editable non-active configuration becomes the active configuration. This action corresponds with the TMA button *Send all attributes to device*: .

When use this action?

Use this action after you made all the necessary configuration settings and you want to activate these settings.

5.6.3 Loading the saved configuration

telindus1031/Load Saved Configuration

If you execute this action, the non-active configuration is overwritten by the active configuration currently used by the Telindus 1031 Router.

After executing this action, click on the TMA button *Retrieve all attributes from device* to see the new non-active configuration.

When use this action?

If you are in the progress of modifying the non-active configuration but made some mistakes, then use this action to revert to the active configuration.

5.6.4 Loading the default configuration using the action

telindus1031/Load Default Configuration

If you execute this action, the non-active configuration is overwritten by the default configuration.

After executing this action, click on the TMA button *Retrieve all attributes from device* to see the new non-active configuration.

When use this action?

If you install the Telindus 1031 Router for the first time, all configuration attributes have their default values. If the Telindus 1031 Router has already been configured but you want to start from scratch, then use this action to revert to the default configuration.

5.6.5 Loading the default configuration using the DIP switch

The following procedure shows how to load the default configuration using the *Load Default Configuration* DIP switch on the Telindus 1031 Router PCB:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 32.</td></tr>
<tr><td>2</td><td>Set DIP switch bank DS2 position 2 to off.
Refer to 3.1 - The Telindus 1031 Router motherboard on page 30 to locate this DIP switch bank.</td></tr>
<tr><td>3</td><td>Replace the cover without fastening the screws and reconnect the power supply.
⇒The Telindus 1031 Router reboots and loads the default configuration.</td></tr>
<tr><td>4</td><td>Activate the loaded default configuration:
<table><tr><th>Step</th><th>Action</th></tr><tr><td>1</td><td>Open a TMA session on the Telindus 1031 Router. Refer to 4.1 - Managing the Telindus 1031 Router with TMA on page 34.</td></tr><tr><td>2</td><td>Execute the Activate Configuration action.[1]</td></tr></table>1. If you are performing this load default configuration procedure because you accidentally made a configuration error, you have the possibility to retrieve this erroneous configuration before executing the Activate Configuration command. In that case you do not have to reconfigure the complete device again, but you only have to correct the error in question. Retrieve the erroneous configuration by executing the Load Saved Configuration command.</td></tr>
<tr><td>5</td><td>Again, disconnect the power supply and open the housing.</td></tr>
<tr><td>6</td><td>Reset DIP switch bank DS2 position 2 to on.</td></tr>
<tr><td>7</td><td>Properly replace the cover as described in 3.3 - Opening and closing the housing on page 32 and reconnect the power supply.</td></tr>
</table>

Always reboot the Telindus 1031 Router after changing the DIP switches.

6 Configuring the WAN encapsulation protocols

This chapter introduces the WAN encapsulation protocols and lists the attributes you can use to configure the encapsulation protocols.

The following gives an overview of this chapter:

- 6.1 - Selecting a WAN encapsulation protocol on page 72
- 6.2 - Configuring PPP encapsulation on page 73
- 6.3 - Configuring Frame Relay encapsulation on page 77
- 6.4 - Configuring ATM encapsulation on page 86
- 6.5 - Configuring HDLC encapsulation on page 95

Refer to the Reference manual on page 169 for a complete overview of the attributes of the Telindus 1031 Router.

6.1 Selecting a WAN encapsulation protocol

First select the encapsulation protocol you want to use on the WAN. Do this using the encapsulation attribute. Refer to telindus1031/g703[ ]/channel[ ]/encapsulation on page 184.

Once you selected a WAN encapsulation protocol you can fine-tune it as described in this chapter.

6.2 Configuring PPP encapsulation

This section introduces the PPP encapsulation protocol and gives a short description of the attributes you can use to configure this encapsulation protocol.

The following gives an overview of this section:

- 6.2.1 - Introducing PPP on page 74
- 6.2.2 - Configuring an IP address on the PPP WAN on page 75
- 6.2.3 - Configuring link monitoring on page 75
- 6.2.4 - Configuring PPP authentication on page 76

6.2.1 Introducing PPP

What is PPP?

The Point-to-Point Protocol (PPP) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for assigning and managing IP addresses, asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for added networking capabilities.

What is LCP, IPCP and BCP?

PPP provides a method for transmitting datagrams over serial point-to-point links, which include the following three components:

- A method for encapsulating datagrams over serial links.
- An extensible Link Control Protocol (LCP) which provides a method of establishing, configuring, maintaining, and terminating the point-to-point connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols such as the IP Control Protocol (IPCP) or the Bridge Control Protocol (BCP).

What is CHAP?

The Telindus 1031 Router also features the Challenge Handshake Authentication Protocol (CHAP). This is a standardised authentication protocol (in compliance with RFC1994) over PPP links. The password is hashed before sending it over the link. The used hashing algorithm is MD5. CHAP authentication over a link can be performed in one direction or in both directions.

The PPP handshake

PPP makes a handshake in two phases:

Phase	Description
1	The Link Control Protocol (LCP) builds the link layer.
2	The IP Control Protocol (IPCP) prepares the exchange of IP packets.

6.2.2 Configuring an IP address on the PPP WAN

When you use PPP encapsulation on the WAN interface, you can configure the IP related parameters using the ip structure in the ppp object.

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

6.2.3 Configuring link monitoring

Refer to 6.2.1 - Introducing PPP on page 74 for an introduction on link monitoring.

The PPP protocol features link monitoring. You can use this to verify whether the WAN link is up or down. If link monitoring is enabled, then the Telindus 1031 Router sends an echo request packet over the line at regular intervals. If on consecutive requests no reply is given, then the PPP link is declared down. Data traffic is stopped until the PPP handshake succeeds again.

You can enable or disable link monitoring and fine-tune it using the linkMonitoring attribute. Refer to telindus1031/g703[ ]/channel[ ]/ppp/linkMonitoring on page 186.

6.2.4 Configuring PPP authentication

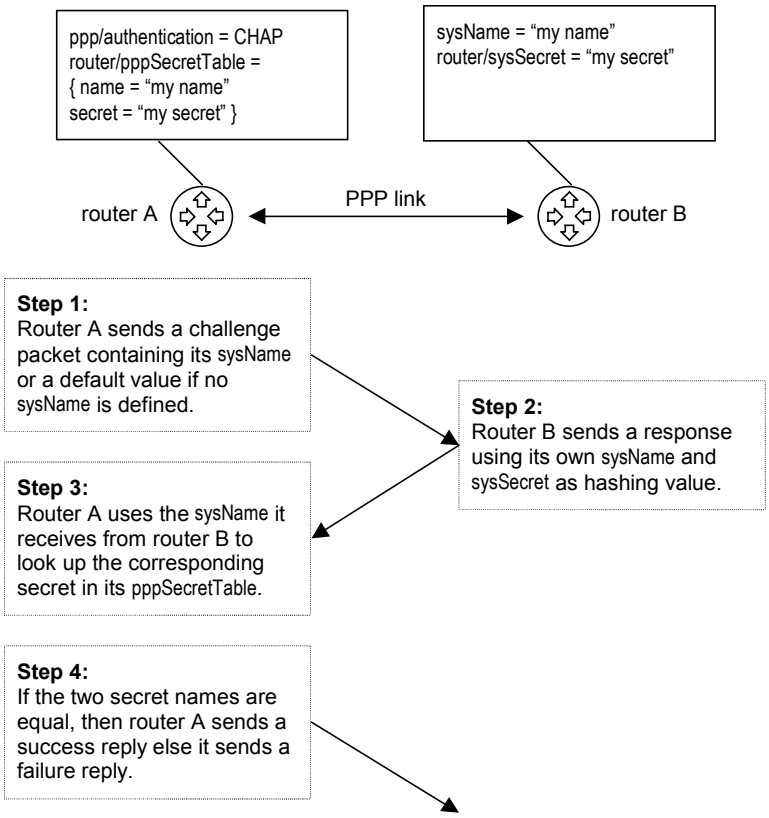
Refer to 6.2.1 - Introducing PPP on page 74 for an introduction on CHAP.

CHAP authentication in one direction

The figure shows CHAP authentication in one direction.

Router A is called the authenticator and the router B is called the peer. Router A is configured for CHAP authentication and the router B is not.

Router A authenticates after building its LCP layer and prior to building the IPCP layer. If the authentication succeeds, then the PPP link is built further until data can be sent. Else PPP starts its handshake again. During data transfer it also authenticates at regular intervals.


ppp/authentication = CHAP
router/pppSecretTable =
{ name = “my name”
secret = “my secret” }
sysName = “my name”
router/sysSecret = “my secret”
router A
PPP link
router B
Step 1:
Router A sends a challenge packet containing its sysName or a default value if no sysName is defined.
Step 2:
Router B sends a response using its own sysName and sysSecret as hashing value.
Step 3:
Router A uses the sysName it receives from router B to look up the corresponding secret in its pppSecretTable.
Step 4:
If the two secret names are equal, then router A sends a success reply else it sends a failure reply.

CHAP authentication in both directions

If CHAP authentication is enabled on both routers, then they both request and respond to the authentication. If the remote router is a router from another vendor, then read the documentation in order to find out how to configure the CHAP name and secret values.

The authentication configuration attributes

As can be seen in the figure above, you have to use the following configuration attributes to configure PPP authentication:

- telindus1031/g703[ ]/channel[ ]/ppp/authentication on page 187
- telindus1031/g703[ ]/channel[ ]/ppp/authenPeriod on page 187
- telindus1031/router/sysSecret on page 207
- telindus1031/router/pppSecretTable on page 207

6.3 Configuring Frame Relay encapsulation

This section introduces the Frame Relay encapsulation protocol and gives a short description of the attributes you can use to configure this encapsulation protocol.

The following gives an overview of this section:

- 6.3.1 - Introducing Frame Relay on page 78
- 6.3.2 - Configuring IP addresses on the Frame Relay WAN on page 80
- 6.3.3 - Configuring the DLCIs on page 83
- 6.3.4 - Configuring LMI on page 84
- 6.3.5 - Configuring CIR and EIR on page 85

6.3.1 Introducing Frame Relay

What is Frame Relay?

Frame Relay is a networking protocol that works at the bottom two levels of the OSI reference model: the physical and data link layers. It is an example of packet-switching technology, which enables end stations to dynamically share network resources.

Frame Relay devices fall into the following two general categories:

- Data Terminal Equipment (DTEs), which include terminals, personal computers, routers, and bridges.
- Data Circuit-terminating Equipment (DCEs), which transmit the data through the network and are often carrier-owned devices.

What is DLCI?

Frame Relay networks transfer data using one of the following connection types:

- Switched Virtual Circuits (SVCs), which are temporary connections that are created for each data transfer and then are terminated when the data transfer is complete (not a widely used connection).
- Permanent Virtual Circuits (PVCs), which are permanent connections.

The Telindus 1031 Router makes use of Permanent Virtual Circuits. The Data Link Connection Identifier (DLCI) is a value assigned to each virtual circuit and DTE device connection point in the Frame Relay WAN. Two different connections can be assigned the same value within the same Frame Relay WAN, one on each side of the virtual connection.

What is LMI?

A set of Frame Relay enhancements exists, called the Local Management Interface (LMI). The LMI enhancements offer a number of features (referred to as extensions) for managing complex networks, including:

- global addressing,
- virtual circuit status messages,
- multicasting.

What is CIR?

The Committed Information Rate (CIR) is the specified amount of guaranteed bandwidth (measured in bits per second) on a Frame Relay service. Typically, when purchasing a Frame Relay service the customer can specify the CIR level he wishes. The Frame Relay network provider guarantees that traffic not exceeding this level will be delivered.

What is EIR?

The Excess Information Rate (EIR) is the specified amount of unguaranteed bandwidth (measured in bits per second) on a Frame Relay service. It is the traffic in excess of the CIR. This traffic may also be delivered, but this is not guaranteed. Obviously, the maximum possible EIR is the physical speed of the customer's access circuit into the Frame Relay service provider.

What is the Discard Eligible bit?

When the CIR is exceeded, all subsequent frames get marked Discard Eligible by setting the DE bit in the Frame Relay header. This is performed at the local Frame Relay switch. If congestion occurs at a node in the Frame Relay network, packets marked DE are the first to be dropped. Upon detecting congestion, a Frame Relay switch will send a Backward Explicit Congestion Notifier (BECN) message back to the source. If the source (e.g. the router) has sufficient intelligence to process this message, it may throttle back to the CIR.

6.3.2 Configuring IP addresses on the Frame Relay WAN

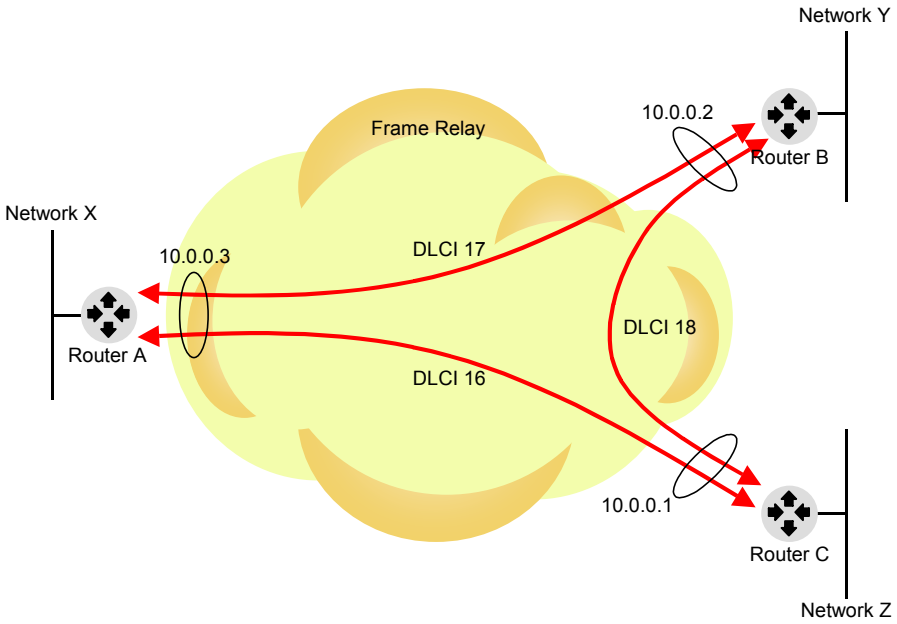
When you use Frame Relay encapsulation on the WAN interface, you can configure the IP related parameters on two levels:

Using the ip structure in the …	Use this structure to configure the IP related parameters of …
frameRelay object.	all the DLCIs for which … • in the dlciTable no IP address is defined for that specific DLCI, • and the mode element is set to routing or routingAndBridgning. In other words, use this attribute to globally configure the IP parameters of the DLCIs. Refer to Example - DLCI global IP.
dlciTable attribute.	one specific DLCI. Refer to Example - DLCI specific IP.

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

Example - DLCI global IP

Suppose you have the following set-up:



If you consider Router A, then for this router …

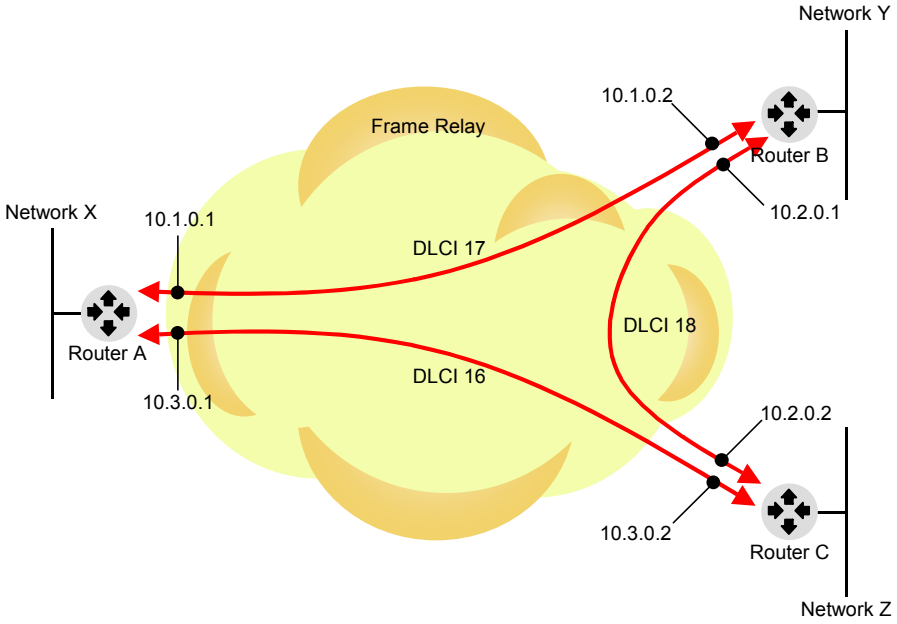
- two DLCIs are configured in the frameRelay/dlciTable, being DLCI 16 and DLCI 17,
- no IP addresses are specifically configured for these DLCIs,
- in the frameRelay/ip attribute a global IP address is configured for the DLCIs, being 10.0.0.3.

The characteristics of a set-up with a global IP address for the DLCIs are:

- Broadcasts are copied and sent over all DLCIs (that use the global IP address). E.g. pinging 10.0.0.255 results in a reply from 10.0.0.1, 10.0.0.2 and 10.0.0.3.
- Pinging 10.0.0.3 results in a reply when LMI is up.
- Routes learned over one DLCI are not passed to other DLCIs. E.g. a route learned over DLCI 16 is not passed to DLCI 17. This means that split horizon is applicable.
- RIP only functions if the network is fully meshed. I.e. if every router is directly connected to its neighbour with a DLCI (as in the example above).

Example - DLCI specific IP

Suppose you have the following set-up:



If you consider Router A, then for this router …

- two DLCIs are configured in the frameRelay/dlciTable, being DLCI 16 and DLCI 17,
- an IP address is specifically configured per DLCI in the frameRelay/dlciTable/ip attribute,
- no global IP address is configured for the DLCIs.

The characteristics of a set-up with a specific IP address for each DLCI are:

- Each DLCI is an IP interface.
- Pinging 10.1.0.1 results in a reply when the DLCI is up.
- Routes learned over one DLCI are passed to other DLCIs. E.g. a route learned over DLCI 16 is passed to DLCI 17. This means that split horizon is not applicable.

6.3.3 Configuring the DLCIs

Refer to 6.3.1 - Introducing Frame Relay on page 78 for an introduction on DLCIs.

Learning the DLCIs

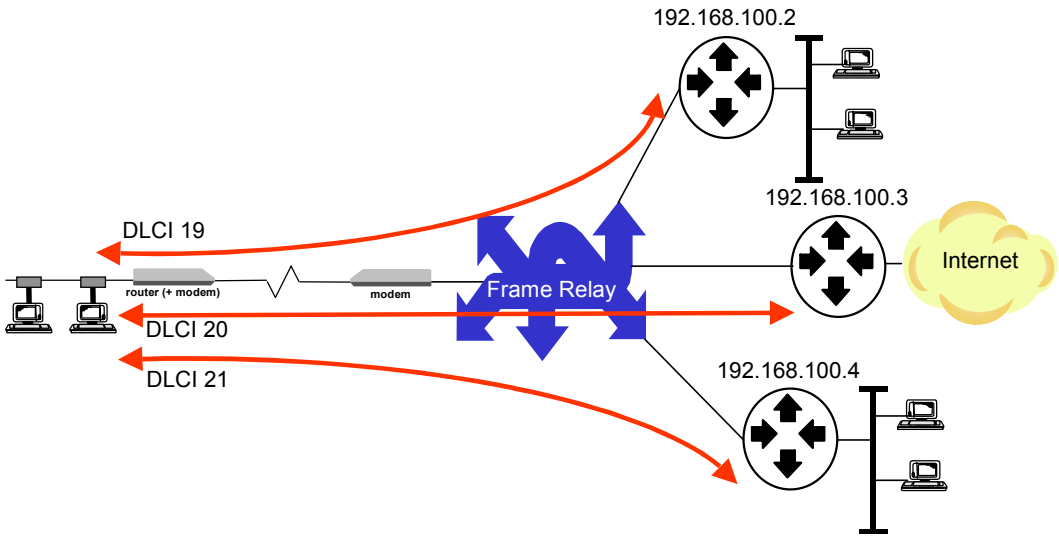
If the Frame Relay network supports LMI, then the Telindus 1031 Router can learn its active and inactive DLCIs. If the Frame Relay network also supports the RARP (Reverse Address Resolution Protocol) protocol, the Telindus 1031 Router can learn the IP address of the corresponding router for each DLCI.

Configuring the DLCIs

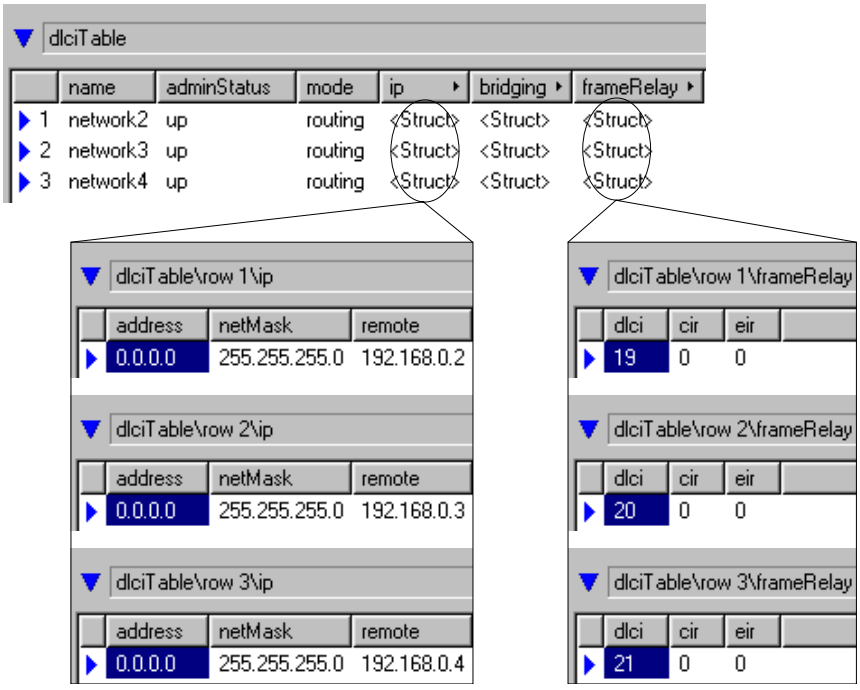
If neither LMI nor RARP is supported by the Frame Relay network you can configure the DLCIs yourself using the dlciTable. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable on page 189.

Example

The following figure gives an example of a local Ethernet segment connected to three different networks through three different DLCIs:



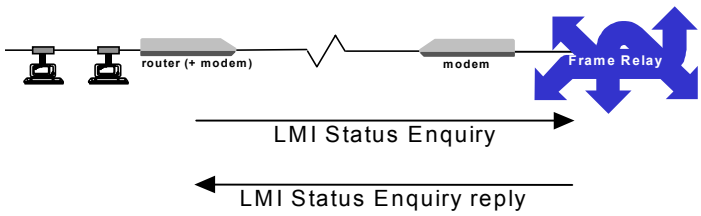
The following screenshot shows (part of) the dlciTable of the set-up depicted in the figure above:



6.3.4 Configuring LMI

Refer to 6.3.1 - Introducing Frame Relay on page 78 for an introduction on LMI.

The LMI provides a status mechanism which gives an on-going status report on the DLCIs. These status reports are exchanged between the Frame Relay access device (or Frame Relay DTE or user) and Frame Relay node (or Frame Relay DCE or network).



At regular intervals, the DTE sends Full Status Enquiry messages to the DCE. The DCE answers with the status of all its DLCIs on the interface. At smaller intervals, the DTE sends Status Enquiry messages. In that case, the DCE only answers with DLCI status changes.

You can select the Local Management Interface (LMI) protocol and fine-tune the LMI operation using the lmi attribute. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/lmi on page 191.

6.3.5 Configuring CIR and EIR

Refer to 6.3.1 - Introducing Frame Relay on page 78 for an introduction on CIR and EIR.

As said before, CIR is the data rate which the user expects to pass into the Frame Relay network with few problems. Note that the CIR is unrelated to the actual bit rate of the physical connection. A user could have a physical connection operating at 2 Mbps, but a CIR across this physical connection of only 64 kbps. This would mean that the user's average data rate would be 64 kbps, but data bursts up to 2 Mbps would be possible (EIR).

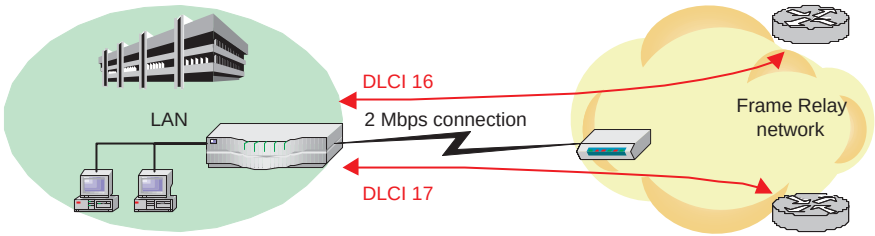
You can configure the CIR and EIR using the cir and eir elements of the frameRelay structure within the dlciTable. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay on page 190.

Important remarks

- Be careful not to over-dimension the CIR. I.e. do not let the sum of the CIRs of the DLCIs exceed the bandwidth of the physical connection.
- When you do exceed the total bandwidth of the physical connection, then the Telindus 1031 Router first buffers the data. However, when the buffers of the Telindus 1031 Router are completely filled up, it has to discard the "excess" data.

Examples

Suppose you have a 2 Mbps physical connection towards the Frame Relay service provider and you define 2 DLCIs:



- Suppose you assign to both DLCIs a CIR of 1 Mbps and an EIR of 0.

  ⇒In that case you have per DLCI a guaranteed bandwidth of 1 Mbps and no bursts are allowed.

- Suppose you assign to both DLCIs a CIR of 512 kbps and an EIR of 512 kbps.

  ⇒In that case you have per DLCI a guaranteed bandwidth of 512 kbps and you allow bursts up to 1 Mbps. This means that if on both DLCIs a burst up to 1 Mbps occurs at the same time, the speed of the physical connection (2 Mbps) is still not exceeded (so no data is discarded). If however somewhere else on the network a congestion occurs, it is possible that some of the "excess" data is discarded (refer to What is the Discard Eligible bit? on page 79).

- Suppose you assign to both DLCIs a CIR of 1 Mbps and an EIR of 1 Mbps.

  ⇒In that case you have per DLCI a guaranteed bandwidth of 1 Mbps and you allow bursts up to 2 Mbps. Obviously, this means that if on both DLCIs a burst up to 2 Mbps occurs at the same time, the speed of the physical connection (2 Mbps) is exceeded and some data is discarded. In that case the principle of first come, first served is applied. I.e. the DLCI on which the burst occurred first its data is passed on to the Frame Relay network. If however somewhere else on the network a congestion occurs, it is still possible that some of the "excess" data is discarded.

- Suppose you assign to both DLCIs a CIR of 2 Mbps and an EIR of 0.

  ⇒In that case you over-dimensioned your CIR. You can not guarantee 2 Mbps of bandwidth for both DLCIs, due to the bandwidth limit of 2 Mbps on the physical connection. Also in this case the principle of first come, first served is applied. I.e. the DLCI which sends data first gets its data onto the Frame Relay network.

6.4 Configuring ATM encapsulation

This section introduces the ATM encapsulation protocol and gives a short description of the attributes you can use to configure this encapsulation protocol.

The following gives an overview of this section:

- 6.4.1 - Introducing ATM on page 87
- 6.4.2 - Configuring IP addresses on the ATM WAN on page 89
- 6.4.3 - Configuring the PVCs on page 90
- 6.4.4 - Configuring the PCR on page 91
- 6.4.5 - Configuring multi-protocol over ATM on page 94
- 6.4.6 - Configuring Classical IP on page 94

6.4.1 Introducing ATM

What is ATM?

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides scalable bandwidth. Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as time-division multiplexing (TDM).

With TDM, each user is assigned to a time slot, and no other station can send in that time slot. If a station has much data to send, it can send only when its time slot comes up, even if all other time slots are empty. However, if a station has nothing to transmit when its time slot comes up, the time slot is sent empty and is wasted. Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell.

What is VPI and VCI?

ATM networks are fundamentally connection-oriented, which means that a virtual channel must be set up across the ATM network prior to any data transfer. (A virtual channel is roughly equivalent to a Permanent Virtual Circuit or PVC.)

Two types of ATM connections exist:

- virtual paths, which are identified by Virtual Path Identifiers (VPIs).
- virtual channels, which are identified by the combination of a VPI and a Virtual Channel Identifier (VCI).

A virtual path is a bundle of virtual channels, all of which are switched transparently across the ATM network based on the common VPI. All VPIs and VCIs, however, have only local significance across a particular link and are remapped, as appropriate, at each switch.

How does ATM switching work?

The basic operation of an ATM switch is straightforward:

The cell is received across a link on a known VCI or VPI value. The switch looks up the connection value in a local translation table to determine the outgoing port (or ports) of the connection and the new VPI/VCI value of the connection on that link. The switch then retransmits the cell on that outgoing link with the appropriate connection identifiers. Because all VCIs and VPIs have only local significance across a particular link, these values are remapped, as necessary, at each switch.

What are the ATM layers?

The ATM reference model is composed of the following ATM layers:

Layer	Description
physical layer	Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.
ATM layer	Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.
ATM Adaptation Layer (AAL)	Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.
higher layers	Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL.

What is multi-protocol over ATM?

As its name implies, multi-protocol encapsulation over ATM provides mechanisms for carrying traffic other than just IP. There are two ways to do this:

Layer	Description
Logical Link Control (LLC) encapsulation	In this method, multiple protocol types can be carried across a single connection with the type of encapsulated packet identified by a standard LLC/SNAP header.
Virtual connection multiplexing	In this method, only a single protocol is carried across an ATM connection, with the type of protocol implicitly identified at connection setup.

LLC encapsulation is provided to support routed and bridged protocols. In this encapsulation format, PDUs from multiple protocols can be carried over the same virtual connection. The type of protocol is indicated in the packet's SNAP header. By contrast, the virtual connection multiplexing method allows for transport of just one protocol per virtual connection.

6.4.2 Configuring IP addresses on the ATM WAN

When you use ATM encapsulation on the WAN interface, you can configure the IP related parameters per PVC using the ip attribute in the pvcTable.

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

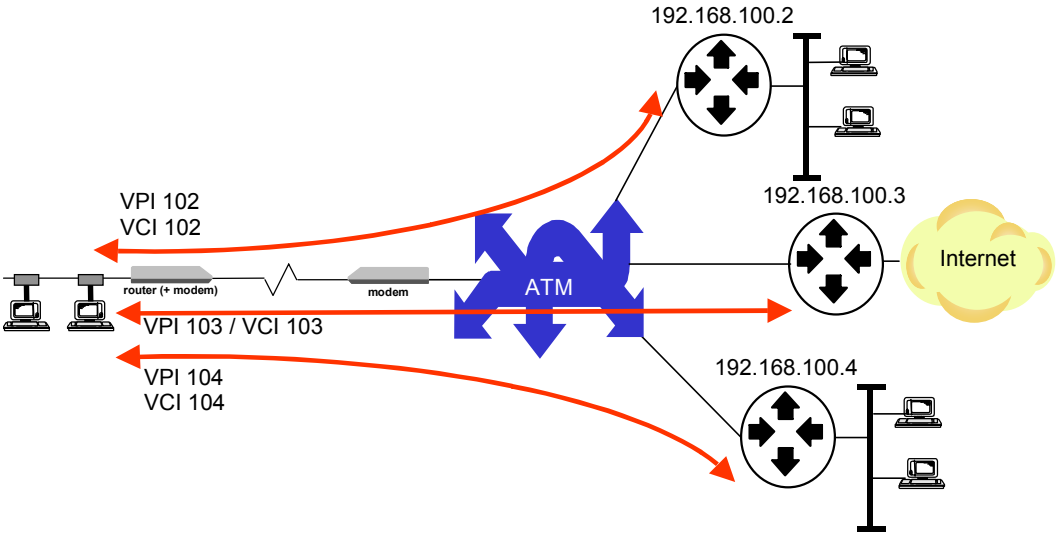
6.4.3 Configuring the PVCs

Refer to 6.4.1 - Introducing ATM on page 87 for an introduction on PVC, VPI and VCI.

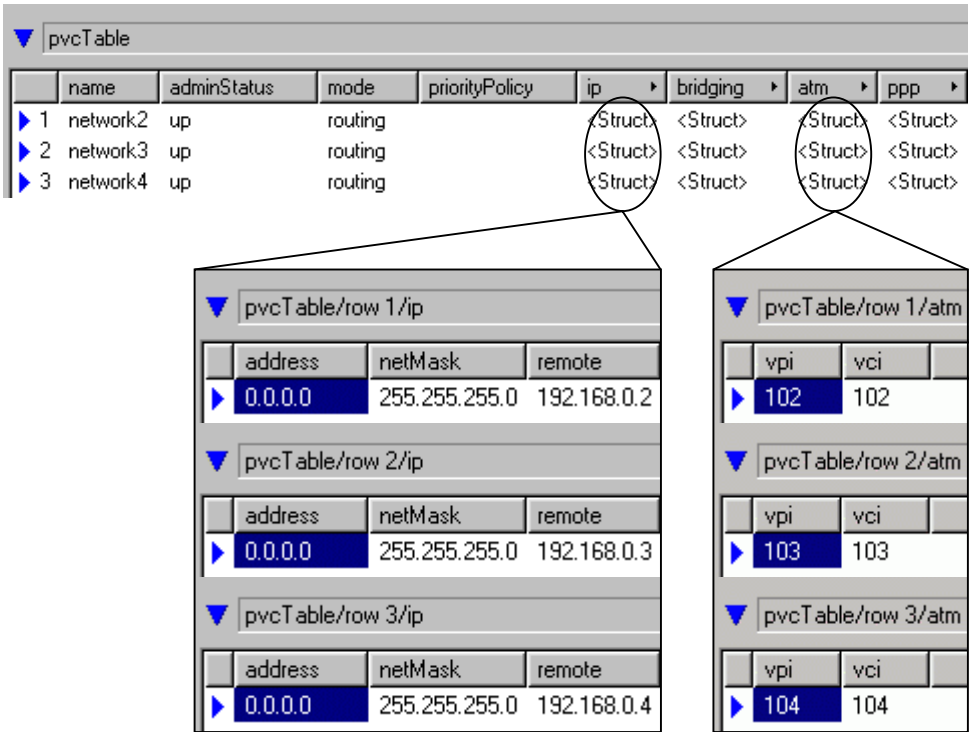
Somewhat similar to the DLCIs in a Frame Relay network (refer to 6.3.3 - Configuring the DLCIs on page 83), you can set-up PVCs in the ATM network. A PVC allows direct connectivity between sites. In this way, a PVC is similar to a leased line. A PVC guarantees availability of a connection and does not require call setup procedures between switches. Use the pvcTable to set up (a) PVC(s). Refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable on page 193.

Example

The following figure gives an example of a local Ethernet segment connected to three different networks through three different PVCs:



The following screenshot shows (part of) the pvcTable of the set-up depicted in the figure above:



6.4.4 Configuring the PCR

The Peak Cell Rate (PCR) is comparable to the EIR in Frame Relay (refer to What is EIR? on page 78). In other words, it is the specified amount of unguaranteed bandwidth (measured in bits per second) on an ATM service. Refer to the Important remarks below to see how to set a guaranteed bandwidth.

The major difference between the PCR mechanism on ATM and the CIR/EIR mechanism on Frame Relay (refer to 6.3.5 - Configuring CIR and EIR on page 85) is that in case of ATM the bandwidth assigned to each PVC is recalculated at regular intervals. This means that depending on the traffic on the PVCs, the Telindus 1031 Router can (proportionally) divide the bandwidth over the different PVCs. As a result, over-dimensioning the PCR on ATM is not as fatal as over-dimensioning the CIR on Frame Relay. The following examples will clarify this.

To configure the PCR, use the peakCellRate element in the atm structure within the pvcTable. Refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm on page 195.

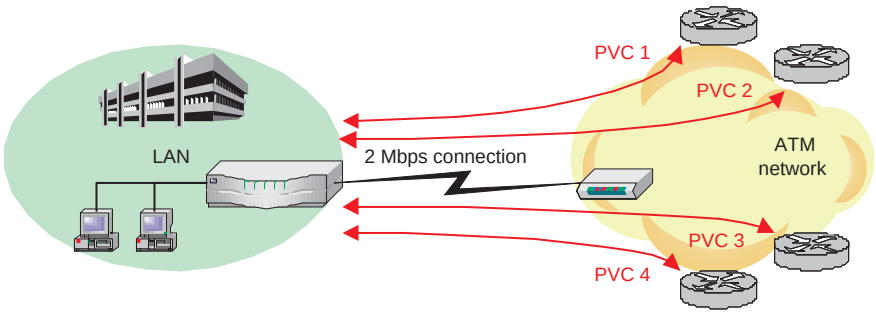
Important remarks

- Per definition, the PCR is the specified amount of unguaranteed bandwidth. However, if you want to set a guaranteed bandwidth, then …
  - do not over-dimension the PCR (i.e. do not let the sum of the PCRs of the PVCs exceed the bandwidth of the physical connection).
  - do not set the PCR to auto.
- When you do exceed the total bandwidth of the physical connection, then the Telindus 1031 Router first buffers the data. However, when the buffers of the Telindus 1031 Router are completely filled up, it has to discard the “excess” data.

Examples

Suppose you have a 2 Mbps physical connection towards the ATM service provider and you define 4 PVCs:

The following tables show some possible scenarios.



Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	auto	2048 kbps	512 kbps
PVC 2	auto	2048 kbps	512 kbps
PVC 3	auto	2048 kbps	512 kbps
PVC 4	auto	2048 kbps	512 kbps

⇒Because all PCRs are set to auto, each PVC tries to get a maximum bandwidth. Hence, the total available bandwidth (2 Mbps) is divided equally over the four PVCs.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	auto	2048 kbps	512 kbps
PVC 2	auto	1024 kbps	512 kbps
PVC 3	auto	640 kbps	512 kbps
PVC 4	auto	512 kbps	512 kbps

⇒Because all PCRs are set to auto, each PVC tries to get a maximum bandwidth. Hence, the total available bandwidth (2 Mbps) is divided equally over the four PVCs. So in this scenario, PVC 3 is the only one that gets all of its data on the ATM network.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	auto	2048 kbps	2048 kbps
PVC 2	auto	0	0
PVC 3	auto	0	0
PVC 4	auto	0	0

⇒Because PVC 1 is the only one sending data and because its PCR is set to auto, it gets the total available bandwidth (2 Mbps) and is able to send its data at 2048 kbps.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	2048 kbps	2048 kbps	1024 kbps
PVC 2	1024 kbps	2048 kbps	512 kbps
PVC 3	512 kbps	2048 kbps	256 kbps
PVC 4	512 kbps	2048 kbps	256 kbps

⇒In this case the PCRs of the PVCs are over-dimensioned (i.e. the sum of the PCRs exceeds the bandwidth of the physical connection towards the ATM network). What is more, the total amount of data that the PVCs try to send also exceeds the total amount of available bandwidth.
As a result, the total available bandwidth (2 Mbps) is divided proportionally over the PVCs:
2048 kbps is the total available bandwidth and 512 kbps is the lowest speed. So PVC 1 gets 4/8th (1024 kbps) of the total available bandwidth, PVC 2 gets 2/8th (512 kbps), PVC 3 and 4 each get 1/8th (256 kbps).

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	1024 kbps	2048 kbps	1024 kbps
PVC 2	512 kbps	2048 kbps	512 kbps
PVC 3	448 kbps	2048 kbps	448 kbps
PVC 4	64 kbps	2048 kbps	64 kbps

⇒Because the sum of the PCRs equals the total available bandwidth (2 Mbps), all the PVCs get the bandwidth that is specified in their PCRs.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	2048 kbps	2048 kbps	896 kbps
PVC 2	2048 kbps	2048 kbps	896 kbps
PVC 3	512 kbps	2048 kbps	192 kbps
PVC 4	1024 kbps	64 kbps	64 kbps

⇒In this case the PCRs of the PVCs are over-dimensioned (i.e. the sum of the PCRs exceeds the bandwidth of the physical connection towards the ATM network). What is more, the total amount of data that the PVCs try to send also exceeds the total amount of available bandwidth. However, one PVC (PVC 4) does not use the bandwidth as specified in its PCR.
As a result, the total available bandwidth (2 Mbps) is divided proportionally over the PVCs. The “spare” bandwidth that PVC 4 does not use is also proportionally divided over the three PVCs which can use this extra bandwidth (PVC 1, 2 and 3).

6.4.5 Configuring multi-protocol over ATM

Refer to 6.4.1 - Introducing ATM on page 87 for an introduction on multi-protocol over ATM.

In order to configure multi-protocol over ATM, use the element …

- higherLayerProtocol to define *which protocol*
- multiProtocolMech to define *how the protocol*

… has to be mapped onto ATM Adaptation Layer 5 (AAL5).

Refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm on page 195.

6.4.6 Configuring Classical IP

Classical IP (RFC1577) is one of the first commonly used encapsulations of IP over ATM. The encapsulation method is the same as described in RFC2684 (formerly RFC1483). The IP traffic is encapsulated without Ethernet header. Reverse ARP is in use for the resolution of IP addresses to PVC channels.

In order to configure Classical IP, use the following elements:

- Set the mode element to routing for the relevant PVC (refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable on page 193).
- Set the higherLayerProtocol to rfc2684 for the relevant PVC (refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm on page 195).
- Set the multiProtocolMech to vcMultiplexing for the relevant PVC (refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm on page 195).

Note that Reverse ARP is always in use. Therefore there is no dedicated attribute to enable or disable RARP.

6.5 Configuring HDLC encapsulation

This section introduces the HDLC encapsulation protocol and gives a short description of the attributes you can use to configure this encapsulation protocol.

The following gives an overview of this section:

- 6.5.1 - Introducing HDLC on page 96
- 6.5.2 - Configuring HDLC on page 96

6.5.1 Introducing HDLC

High-level Data Link Control (HDLC) encapsulation means that the Ethernet frames are put in an HDLC frame without any additional encapsulation (such as Frame Relay or PPP). This means that there is no protocol which monitors the status of the link, but it also means that there is no encapsulation overhead.

Because the Ethernet frames are directly encapsulated, only bridging is possible.

Important remark

The HDLC encapsulation on the Telindus 1031 Router is compatible with the HDLC encapsulation on the Crocus Bridge interface. It is however not compatible with the Cisco HDLC encapsulation.

6.5.2 Configuring HDLC

The only thing that is configurable for the HDLC encapsulation protocol is the attribute telindus1031/g703[ ]/channel[ ]/hdlc/bridging on page 199.

7 Configuring the router

This chapter introduces routing on the Telindus 1031 Router and lists the attributes you can use to configure routing. It also introduces the most important features of the router besides routing and lists the attributes you can use to configure these features.

The following gives an overview of this chapter:

- 7.1 - Introducing routing on page 98
- 7.2 - Configuring static routes on page 100
- 7.3 - Configuring the Routing Information Protocol on page 107
- 7.4 - Configuring address translation on page 116
- 7.5 - Configuring L2TP tunnelling on page 127
- 7.6 - Configuring traffic and priority policy on the router on page 130
- 7.7 - Configuring an extended access list on page 138

Refer to the Reference manual on page 169 for a complete overview of the attributes of the Telindus 1031 Router.

7.1 Introducing routing

What is routing?

Routing is the act of moving information across an internetwork from a source to a destination.

Routing versus bridging

Routing is often contrasted with bridging. At first sight, bridging might seem to do the same as routing. The primary difference between the two is that bridging occurs at layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). In other words, bridging occurs at a lower level and is therefore more of a hardware function whereas routing occurs at a higher level where the software component is more important. And because routing occurs at a higher level, it can perform more complex analysis to determine the optimal path for the packet.

Basic routing activities

Routing involves two basic activities:

- determining optimal routing paths,
- transporting information groups (typically called packets).

Determining the optimal routing path

In order to determine a routing path, routers initialise and maintain routing tables. These routing tables contain a variety of information. For example:

- Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.
- Desirability of a path. Routers use metrics to evaluate what path will be the best for a packet to travel.

Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analysing routing updates from all other routers, a router can build a detailed picture of network topology.

Transporting packets

In most cases, a host determines that it must send a packet to another host. Having acquired a router's address by some means, the source host sends a packet addressed specifically to a router's physical (i.e. Media Access Control or MAC) address, this time with the protocol (i.e. network) address of the destination host.

As it examines the packet's destination protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, however, it changes the destination physical address to that of the next hop and transmits the packet.

The next hop may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the internetwork, its physical address changes, but its protocol address remains constant.

Static versus dynamic routing

The following table states the differences between static and dynamic routing:

Routing algorithm	Description
static	Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Static routing algorithms work well in environments where network traffic is relatively predictable and where network design is relatively simple.
dynamic	Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, constantly changing networks. Most of the dominant routing algorithms today are dynamic routing algorithms, which adjust to changing network circumstances by analysing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly. Also refer to 7.3.1 - Introducing RIP on page 108.
static and dynamic	Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way.

7.2 Configuring static routes

This section introduces static routing and gives a short description of the attributes you can use to configure static routing.

The following gives an overview of this section:

- 7.2.1 - Configuring static routes on page 101
- 7.2.2 - Configuring the routing table on page 102
- 7.2.3 - Configuring static routes - examples on page 103
- 7.2.4 - The rerouting principle on page 106

7.2.1 Configuring static routes

Refer to 7.1 - Introducing routing on page 98 for an introduction on routing.

Static routes versus RIP

You have to determine whether you are going to use static routes or the RIP routing protocol:

If your network …	then …
exclusively uses the RIP routing protocol,	you may skip this section. Proceed with 7.3 - Configuring the Routing Information Protocol on page 107.
does not use the RIP routing protocol, or only part of it does,	read this section to learn how to define static routes to the remote IP networks that have to be reached.

The static routing configuration attributes

Use the following to configure static routes:

- Use the routingTable attribute to specify routing entries for specific networks. Refer to …
  - telindus1031/router/routingTable on page 202
  - 7.2.2 - Configuring the routing table on page 102 for more information on the behaviour of the routing table when configuring it.
- Use the defaultRoute attribute to specify a default route (also called gateway). Packets for destinations that do not match one of the routing table entries are sent to this default route. Refer to telindus1031/router/defaultRoute on page 201.

If you only have to reach one remote LAN network from your local Ethernet via this router, you may skip the routingTable attribute. In that case it is sufficient to define the defaultRoute attribute only.

7.2.2 Configuring the routing table

The following are some rules when configuring the routingTable:

Rule	Description
1	As a rule of thumb, one can say that the interface name has priority over the gateway.
2	In case you enter a correct (i.e. existing) interface name and in case it refers to a … • point-to-point (PTP) interface, the route is always added to the routing table, no matter which gateway (GW) is specified. • multi-point (MP) interface, then … - the route is only added to the routing table when a local gateway is specified. - the route is not added to the routing table when no gateway is specified. - a reroute occurs when no local gateway is specified.
3	In case you enter an incorrect interface name, the route is not added to the routing table.
4	In case you enter no interface name then … • the route is added to the routing table when a local gateway is specified. • the route is not added to the routing table when no gateway is specified. • the route is not added to the routing table when the gateway lies within the configured network route. For example: network = 10.0.0.0; mask = 255.255.255.0; gateway = 10.0.0.1. • a reroute occurs when no local gateway is specified.

The following table summarises the above:

Interface name	Gateway	Result
correct	none (0.0.0.0)	• PTP: route added • MP: route not added
correct	local	route added (always)
correct	not local	• PTP: route added[1] • MP: rerouted
incorrect	-	route not added
no name	local for an interface	routed added
no name	not local for an interface Exception: • GW = none (0.0.0.0) • GW lies in configured network route	rerouted to gateway • route not added • route not added

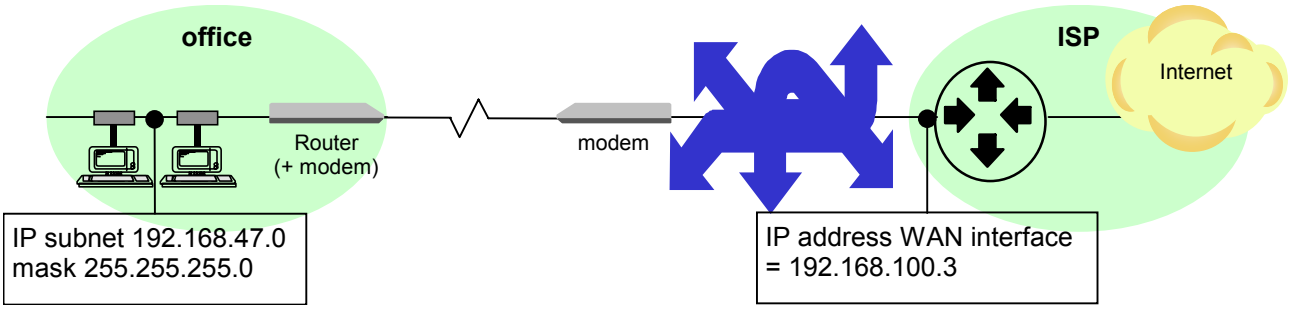
1. In the routingTable status, the configured gateway will appear but for the routing itself the gateway is ignored.

7.2.3 Configuring static routes - examples

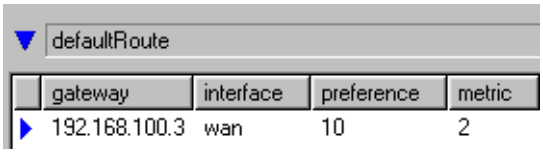
This section presents the following examples:

- Example of a default route on page 103
- Example 1: Static IP route with an IP address on the WAN interface on page 104
- Example 2: Static IP route without an IP address on the WAN interface on page 105

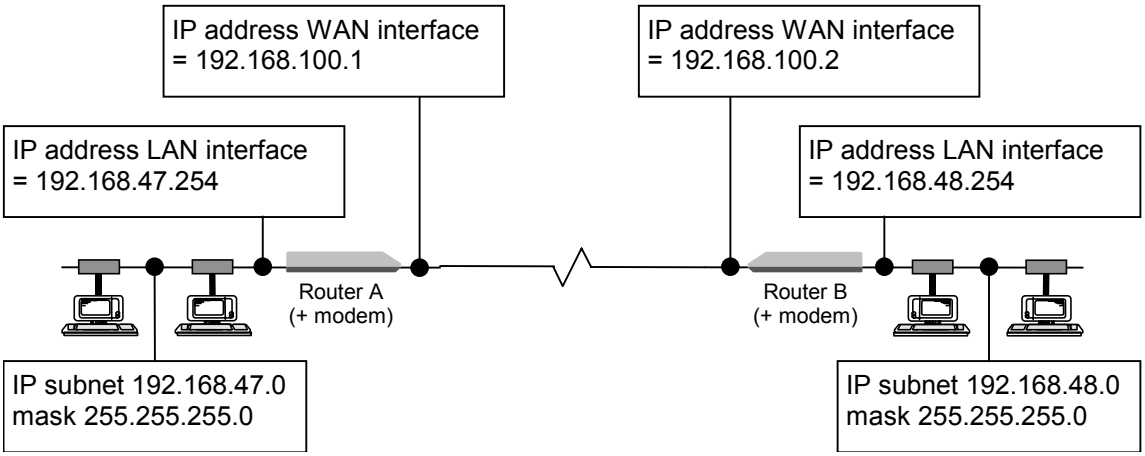
Example of a default route



In this example, an office is connected via a modem link over a network of an operator to an Internet Service Provider (ISP). The Telindus 1031 Router in the office does not need any static routes. All traffic is sent to the ISP. Hence, the Telindus 1031 Router its default route is towards the Internet:



Example 1: Static IP route with an IP address on the WAN interface



In this example, two LANs are interconnected via a modem link. The two routers have an IP address on their WAN interface. To make network 192.168.48.0 reachable from network 192.168.47.0 and vice versa, you have to define one static route in router A (left) and one static route in router B (right) as follows:

Router A:

routingTable

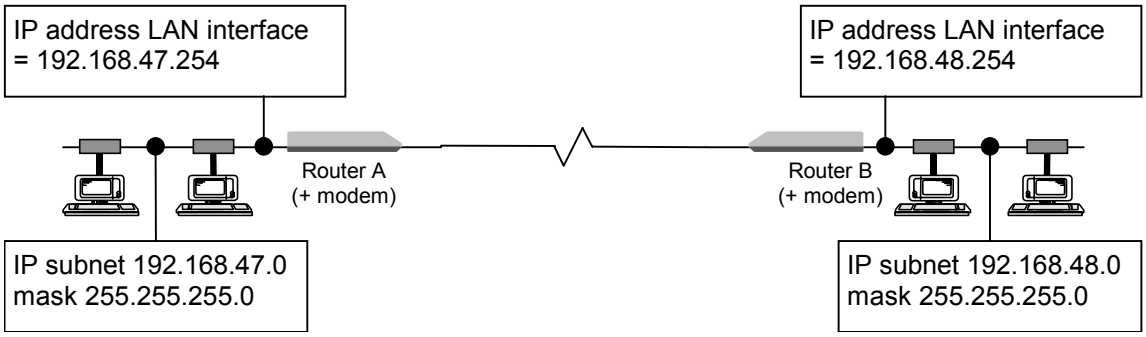
	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.100.2		10	2

Router B:

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.100.1		10	2

Example 2: Static IP route without an IP address on the WAN interface



This example is similar to the previous one, except that now the WAN interfaces do not have an IP address. To make network 192.168.48.0 reachable from network 192.168.47.0 and vice versa, you have to define one static route in router A (left) and one static route in router B (right) as follows:

Router A:

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.48.254	wan	10	2

Router B:

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.47.254	wan	10	2

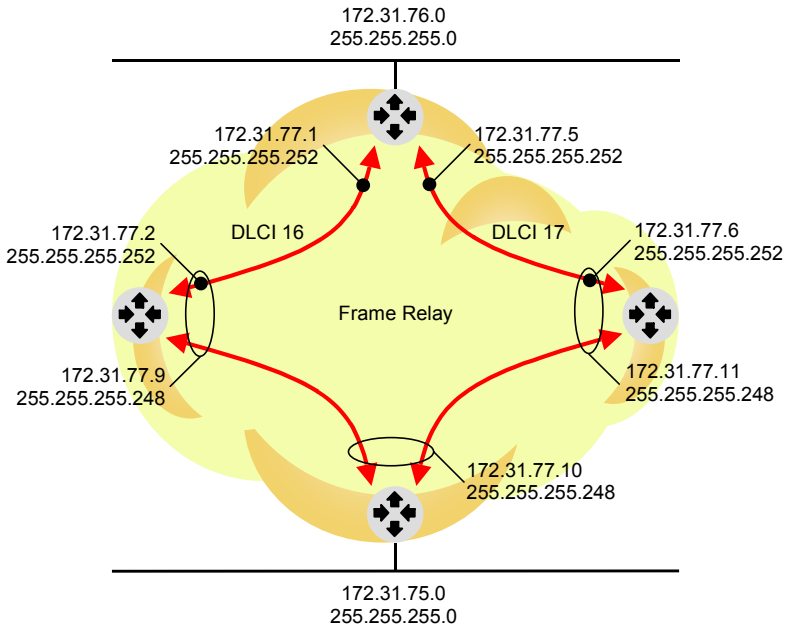
7.2.4 The rerouting principle

What is the rerouting principle?

If the gateway of a route does not belong to the subnet of an interface, then the Telindus 1031 Router adds a special route. Then a second route look-up occurs, this time using the gateway field of the route. This can be used as a back-up functionality as shown below.

Example

Suppose you have the following set-up:



In the routing table, the following routes are defined:

- network 172.31.75.0 is reachable via 172.31.77.10
- 172.31.77.10 is reachable via DLCI 16 (172.31.77.2)
- 172.31.77.10 is also reachable via DLCI 17 (172.31.77.6)

routingTable

	network	mask	gateway	interface	preference	metric
1	172.31.75.0	255.255.255.0	172.31.77.10		10	2
2	172.31.77.10	255.255.255.248	172.31.77.2	wan	10	2
3	172.31.77.10	255.255.255.248	172.31.77.6	wan	10	2

Now in order to reach network 172.31.75.0, DLCI 16 is used. However, when DLCI 16 goes down, the Telindus 1031 Router automatically uses DLCI 17 in order to reach network 172.31.75.0. I.e. it automatically “reroutes” and this without the need of a routing protocol.

Important remarks

- This only works for the entries of the routing table, *not* for the default gateway.
- This type of route is always up.
- In the status information, the interface element of such a route displays internal.

7.3 Configuring the Routing Information Protocol

This section introduces the Routing Information Protocol (RIP) and gives a short description of the attributes you can use to configure RIP.

The following gives an overview of this section:

- 7.3.1 - Introducing RIP on page 108
- 7.3.2 - Configuring RIP on page 109
- 7.3.3 - Explaining the rip structure on page 110
- 7.3.4 - Configuring RIP authentication on page 115

7.3.1 Introducing RIP

What is RIP?

The Routing Information Protocol (RIP) is a protocol that routers use to exchange dynamic routing information.

How does RIP work?

When RIP is enabled, the Telindus 1031 Router advertises every 30 seconds its routing information to adjacent routers. It also receives the routing information from the adjacent routers. With this information it adapts its routing table dynamically. If after 180 seconds no information about a certain route has been received, then this route is declared *down*. If after an additional 120 seconds (i.e. 300 seconds in total) still no information about the route has been received, then this route is deleted from the routing table.

RIP support

The Telindus 1031 Router supports RIP protocol version 1, 1-compatible and 2. RIP version 1 is a very common routing protocol. Version 2 includes extra features like variable subnet masks and authentication. Check which RIP version is used by the other routers in the network.

Currently, the RIPv2 routing protocol requires the use of an IP address on the WAN interface.

7.3.2 Configuring RIP

Refer to …

- 7.1 - Introducing routing on page 98 for an introduction on routing.
- 7.3.1 - Introducing RIP on page 108 for an introduction on RIP.

Use the following to configure RIP:

- First, use the routingProtocol attribute to activate the general RIP process on the Telindus 1031 Router. Refer to telindus1031/router/routingProtocol on page 203.
- Then use the rip structure within the ip structure to configure for each interface the RIP version, the RIP behaviour and to fine-tune the RIP operation. Refer to …
  - 5.2.2 - Where to find the IP related parameters on page 57 for the location of the ip structure. The rip structure is located within the ip structure.
  - 7.3.3 - Explaining the rip structure on page 110 for a detailed explanation of the rip structure.

7.3.3 Explaining the rip structure

Because the rip structure occurs in several objects, it is described here once and referenced where necessary. The rip structure is located within the ip structure. Refer to 5.2.2 - Where to find the IP related parameters on page 57 for the location of the ip structure.

The rip structure contains the following elements:

Element	Description
metric	Use this element to determine with how much the Telindus 1031 Router increments the metric parameter of a route. Default:1 Range: 1 … 15 Routing information includes a metric parameter. Every time a router is passed, this parameter is incremented. Also the Telindus 1031 Router increments the metric parameter (default by 1) before it writes the route in the routing table. Hence, the metric parameter indicates for each route how many routers have to be passed before reaching the network. When several routes to a single network exist and they all have the same preference, then the route with the smallest metric parameter is chosen. However, using the metric element, you can increment the metric parameter by more than 1 (up to a maximum of 15). You could do this, for instance, to indicate that a certain interface is less desirable to route through. As a result, the Telindus 1031 Router adds this value to the metric parameter of every route learnt through that interface. The metric parameter is also used to represent the directly connected subnets on the LAN and WAN interfaces.
mode	Use this element to set the transmission and/or reception of RIP updates on the interface. By default the Telindus 1031 Router transmits and receives RIP updates on all interfaces. Default:active Range: enumerated, see below The mode element has the following values: **Value** / **Description** active — RIP updates are transmitted and received on this interface. passive — RIP updates are not transmitted on this interface, but received updates are parsed. disabled — RIP updates are nor transmitted nor received on this interface.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>txVersion</td><td>Use this element to set the version of the RIP updates that are transmitted on the interface.
Default:rip2
Range: enumerated, see below

The txVersion element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>rip1</td><td>The transmitted RIP updates are RIP version 1 updates.</td></tr>
<tr><td>rip2</td><td>The transmitted RIP updates are RIP version 2 updates.</td></tr>
<tr><td>rip1-compatible</td><td>The contents of the RIP update packet is a RIP version 2 packet, but it is encapsulated as a RIP version 1 packet. This allows some older implementations of RIP 1 to be interoperable with RIP 2.</td></tr>
</table></td></tr>
<tr><td>rxVersion</td><td>Use this element to set which version of received RIP updates is accepted on the interface.
Default:rip2only
Range: enumerated, see below

The rxVersion element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>rip1only</td><td>Only RIP version 1 received RIP updates are accepted.</td></tr>
<tr><td>rip2only</td><td>Only RIP version 2 received RIP updates are accepted.</td></tr>
<tr><td>rip1&2</td><td>Both RIP version 1 and 2 received RIP updates are accepted.</td></tr>
</table>

If you want to accept RIP1-compatible updates on the interface, then set the rxVersion attribute to rip1&2.</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>splitHorizon</td><td>Use this element to enable or disable split horizon operation.
Default:poisonedReverse
Range: enumerated, see below

The splitHorizon element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>Split horizon is disabled.</td></tr>
<tr><td>enabled</td><td>Split horizon is enabled.

Split horizon operation prevents that routing information exits the interface through which the information was received in the first place. This optimises communications among multiple routers, particularly when links are broken. It also prevents routing loops.</td></tr>
<tr><td>poisonedReverse</td><td>Poisoned reverse split horizon is used.

Whereas “simple” split horizon simply omits the routes learned from one neighbour in updates sent to that neighbour, poisoned reverse split horizon includes such routes in updates but sets their metrics to infinity.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>authentication</td><td>Use this element to enable or disable RIP authentication.
Default:disabled
Range: enumerated, see below

Refer to 7.3.4 - Configuring RIP authentication on page 115 for more information on RIP authentication.

The authentication element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>No authentication is used.</td></tr>
<tr><td>text</td><td>The authentication secret is exchanged in clear text.</td></tr>
<tr><td>md5</td><td>Instead of sending the authentication secret together with the RIP updates, it is hashed together with the routing information into a unique value. This authentication is the most secure. This because it provides also protection against tampering with the contents of a packet: both an incorrect password and modified routing information result in different hash values.</td></tr>
</table>

Remarks

• If authentication is enabled (either text or md5), then only updates using that authentication are processed. All other updates on that interface are discarded.
• If you use md5 and if for a certain interface multiple secrets are present in the ripv2SecretTable, then the first entry in the ripv2SecretTable is used to transmit RIP updates. Authentication of the received RIP updates is done by looking for the first secret with a matching key.
• If you use text and if for a certain interface multiple secrets are present in the ripv2SecretTable, then only the first entry in the ripv2SecretTable is used to transmit and receive RIP updates.</td></tr>
</table>

Element	Description
filter	Use this element to apply a filter on the RIP updates on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the filter you want to use. You can create the filter itself by adding a routingFilter object under the router object and by configuring the attributes in this object. **Example** If you created a routingFilter object with index name my_filter (i.e. routingFilter[my_filter]) and you want to apply this filter here, then enter the index name as value for the filter element. Refer to … • 10.5.4 - Routing filter configuration attributes on page 222 for more information on RIP filtering. • 4.4 - Adding an object to the containment tree on page 45 for more information on adding objects.

7.3.4 Configuring RIP authentication

Refer to …

- 7.1 - Introducing routing on page 98 for an introduction on routing.
- 7.3.1 - Introducing RIP on page 108 for an introduction on RIP.

Routers exchange information between each other for management purposes. They do this using the Router Information Protocol (RIP). For security reasons, you can enable RIP authentication. You can do this per interface.

Use the following to configure RIP authentication:

- Use the authentication element in the rip structure to enable RIP authentication per interface. You can also select the authentication method. Refer to 7.3.3 - Explaining the rip structure on page 110.
- Use the ripv2SecretTable attribute to define the secrets used for the RIP authentication. Refer to telindus1031/router/ripv2SecretTable on page 206.

7.4 Configuring address translation

This section explains Network Address Translation (NAT) and Port Address Translation (PAT). Firstly, it gives an introduction. Secondly, a table is presented that will help you to determine which translation method meets your requirements. Then this section teaches you how to configure NAT and PAT.

The following gives an overview of this section:

- 7.4.1 - Introducing NAT and PAT on page 117
- 7.4.2 - When use NAT and/or PAT on page 118
- 7.4.3 - Configuring PAT on page 119
- 7.4.4 - How does PAT work? on page 120
- 7.4.5 - PAT limitations on page 122
- 7.4.6 - PAT limitations workaround on page 123
- 7.4.7 - Configuring NAT on page 124
- 7.4.8 - How does the NAT address table work? on page 125
- 7.4.9 - Combining PAT and NAT on page 126

7.4.1 Introducing NAT and PAT

What is NAT and PAT?

Network Address Translation (NAT) and Port Address Translation (PAT) are used to translate private IP addresses into official IP addresses. This is also known as IP masquerading.

If you use the Telindus 1031 Router to have a permanent connection to the Internet, you may need NAT and/or PAT.

Why use NAT and PAT?

Each device connected to the Internet must have an *official* (i.e. unique) IP address. The success of the Internet has caused a lack of these official IP addresses. As a result, your Internet Service Provider (ISP) may offer you only one or a small number of official IP addresses.

If the number of IP devices on your local network is larger than the number of official IP addresses, you can assign test or private IP addresses to your local network. In that case, you have to configure your Telindus 1031 Router to translate IP addresses using NAT or PAT.

Even when there are sufficient official IP addresses available, you may still choose to use NAT e.g. for preserving previously assigned test addresses to all the devices on your local network.

Private IP address range

The international authority IANA assigns the official (also called global) IP addresses. It has also defined 3 ranges of IP addresses for private use. This means that you can use these addresses without registration on your internal network, as long as you are not connected to the Internet.

Private IP address range	Remarks
10.0.0.0 - 10.255.255.255	1 class A network
172.16.0.0 - 172.31.255.255	16 class B networks
192.168.0.0 - 192.168.255.255	256 class C networks

You can define (sub-)networks in these ranges for your *private IP addresses*.

7.4.2 When use NAT and/or PAT

You can use NAT, PAT or a combination of both:

Address translation	Description
NAT	NAT allows the use of private IP addresses on the local Ethernet, while still having access via the WAN interface to the Internet (official IP addresses). Each Ethernet IP address that needs Internet access is translated into an official IP address before sending traffic on the WAN interface. The number of simultaneous users with Internet access is limited to the number of official IP addresses. This is a dynamic process.
PAT	PAT uses only one single official IP address on the WAN network. The Telindus 1031 Router translates all private IP addresses on the local Ethernet to the single official IP address. Only outgoing TCP sessions are supported.
NAT and PAT	You can combine both translation methods and tune them to specific needs.

Check in the next table whether you need NAT and/or PAT:

No. of official IP addresses	No. of devices on local network	Use NAT of PAT?	Refer to …
1	more than 1	Use PAT.	7.4.3 - Configuring PAT on page 119
k (> 1)	more than k	Use NAT in combination with PAT.	7.4.9 - Combining PAT and NAT on page 126
at least k	k (≥ 1)	1. No translation needed. 2. If you want translation, use NAT.	1. Skip this section. 2. 7.4.7 - Configuring NAT on page 124

7.4.3 Configuring PAT

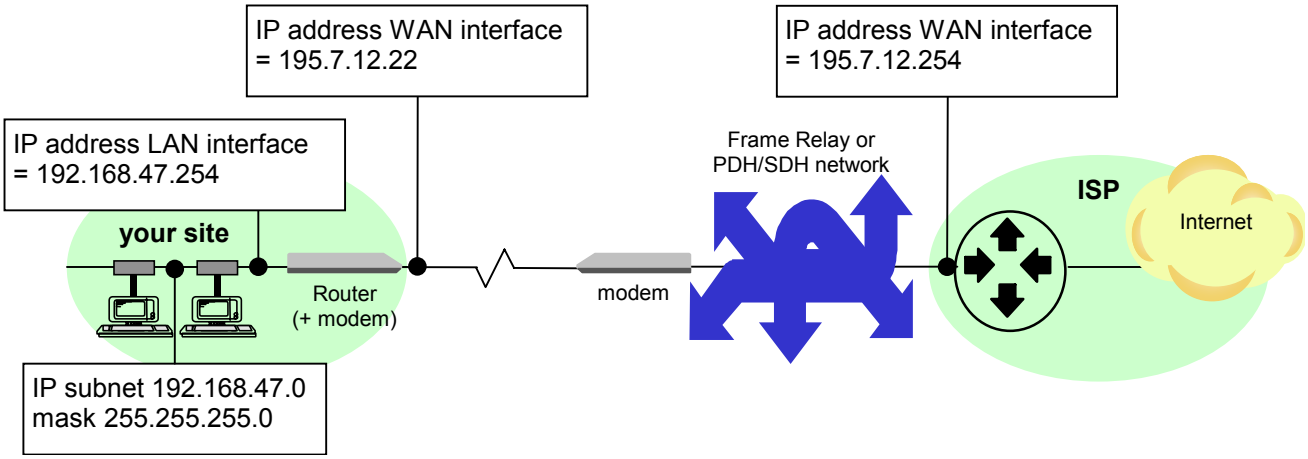
Use the following to configure PAT:

- Use the patAddress attribute to enter official IP address that has to be used for Port Address Translation. Refer to telindus1031/router/defaultNat/patAddress on page 215.
- Use the gateway attribute to define the gateway addresses from routes on which NAT or PAT should be applied. Refer to telindus1031/router/defaultNat/gateway on page 216.

Example of a network topology for Internet connection

Consider the following network topology.

A Telindus 1031 Router is installed at your site. The Internet Service Provider has an IP router with a high speed Frame Relay interface or one or more G.704 framed E1 interfaces running PPP. You received only one single official IP address from you ISP, being 195.7.12.22.



Set IP address 195.7.12.22 to be the PAT address. In this case, it is the same address as on your WAN interface.

The gateway attribute should contain the gateway address 195.7.12.254. However, if you already defined your defaultRoute to be 195.7.12.254, then you can leave the gateway attribute empty. This because if the gateway attribute is empty, then the defaultRoute is taken as only gateway addresses.

7.4.4 How does PAT work?

Again consider the network topology as depicted in 7.4.3 - Configuring PAT on page 119.

The following two paragraphs explain how the Telindus 1031 Router treats the outgoing and incoming traffic when PAT is applied.

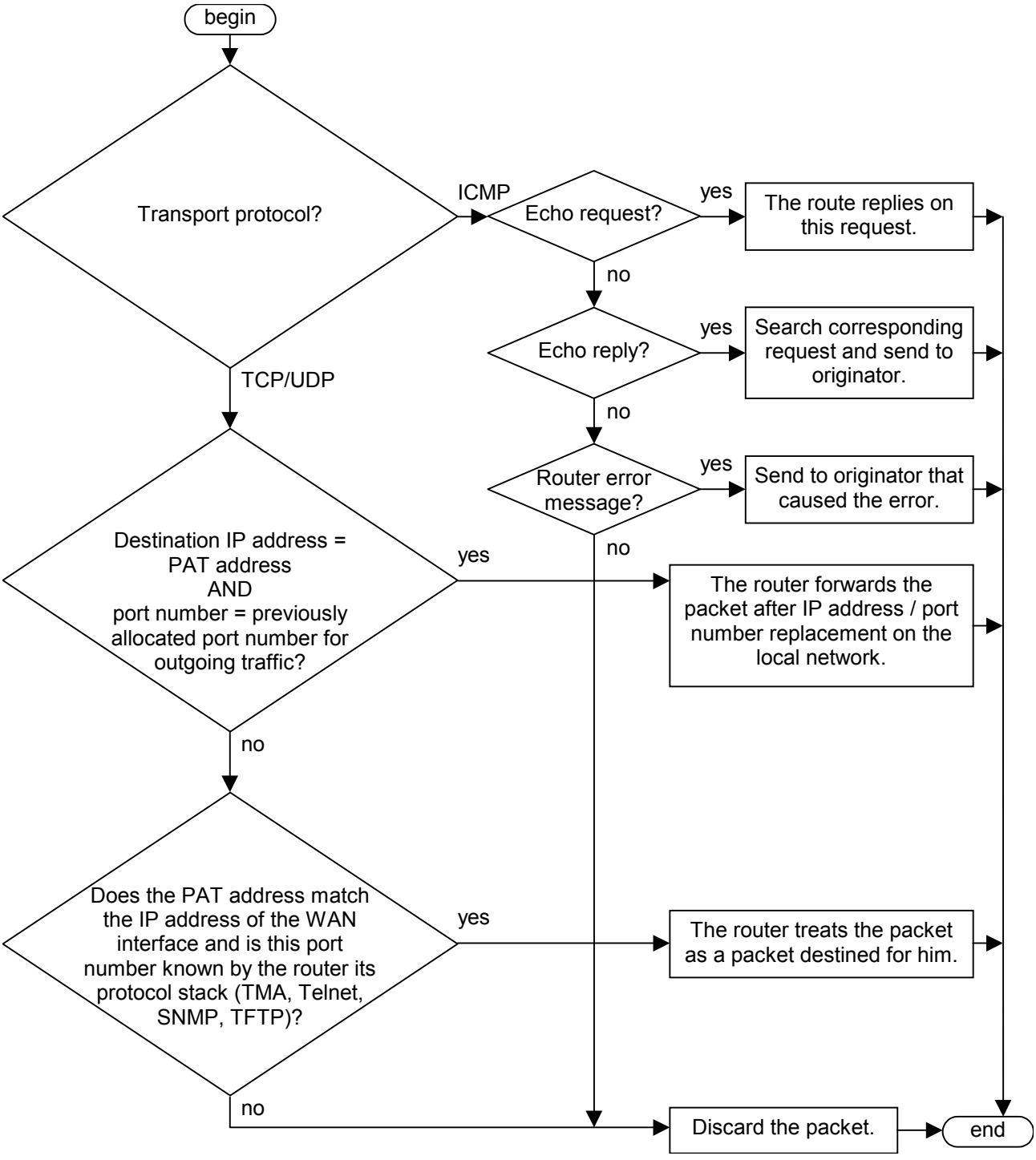
Outgoing traffic (to the Internet)

The Telindus 1031 Router replaces the source address by its PAT address in all the traffic coming from the Ethernet and destined for the Internet. Depending on the IP transport protocol and the number of simultaneous users accessing the Internet, the Telindus 1031 Router takes different actions:

Protocol		
TCP	**Description**	This is a connection-oriented protocol: two devices communicating with the TCP protocol build a session before exchanging user data. When they have finished exchanging user data, the session is closed. Examples of such applications are Telnet, HTTP and FTP. The TCP header contains a *port* field indicating the higher-layer protocol.
	Action	When a session is started, a specific port number is assigned to this session. All traffic from this session is assigned this specific port number. The specific port number is freed within 5 minutes after the TCP session is closed (i.e. after TCP Reset or TCP Finish is seen). If the session has not been properly closed, the port number is freed 24 hours after the last session traffic. This time is configurable (refer to telindus1031/router/defaultNat/tcpSocketTimeOut on page 217).
UDP	**Description**	This is a connection-less protocol: user data can be sent without first building a session. Examples of such applications are SNMP and TFTP. Although TFTP is session-oriented, it builds the session at a higher level and uses UDP for its simplicity as transport protocol. The UDP header contains a *port* field indicating the higher-layer protocol.
	Action	The Source Port Number is replaced by a specific port number. All traffic from this source IP address / port number pair is assigned this specific port number. If there is no traffic for 5 to 10 minutes, the specific port number is freed.
ICMP	**Description**	This is a connection-less protocol: user data can be sent without first building a session. An example of such an application is ping. These protocols do not have port numbers.
	Action	Each ICMP packet is forwarded towards the Internet. Each ICMP packet is considered as a new session. If there is no traffic for 5 to 10 minutes, the session is closed. The fact that it is possible to open a total of 2048 simultaneous sessions and that each ICMP packet is considered as a new session, implies that for instance a continuous series of ping requests at a rate of one per second will allocate between 300 and 600 sessions.

Incoming traffic (from the Internet)

Suppose the WAN IP network depicted in 7.4.3 - Configuring PAT on page 119 works in numbered mode[1]. The incoming traffic from the Internet may be destined either for the local network, or for the Telindus 1031 Router itself. The router treats incoming traffic on the PAT address as follows:


begin
Transport protocol?
ICMP
Echo request?
yes
The route replies on this request.
no
Echo reply?
yes
Search corresponding request and send to originator.
no
Router error message?
yes
Send to originator that caused the error.
no
TCP/UDP
Destination IP address = PAT address AND port number = previously allocated port number for outgoing traffic?
yes
The router forwards the packet after IP address / port number replacement on the local network.
no
Does the PAT address match the IP address of the WAN interface and is this port number known by the router its protocol stack (TMA, Telnet, SNMP, TFTP)?
yes
The router treats the packet as a packet destined for him.
no
Discard the packet.
end

1. Numbered mode means that each WAN interface has an IP address. In that case, you need the single official IP address for your WAN interface.

7.4.5 PAT limitations

Example of PAT and multiple remote networks over Frame Relay

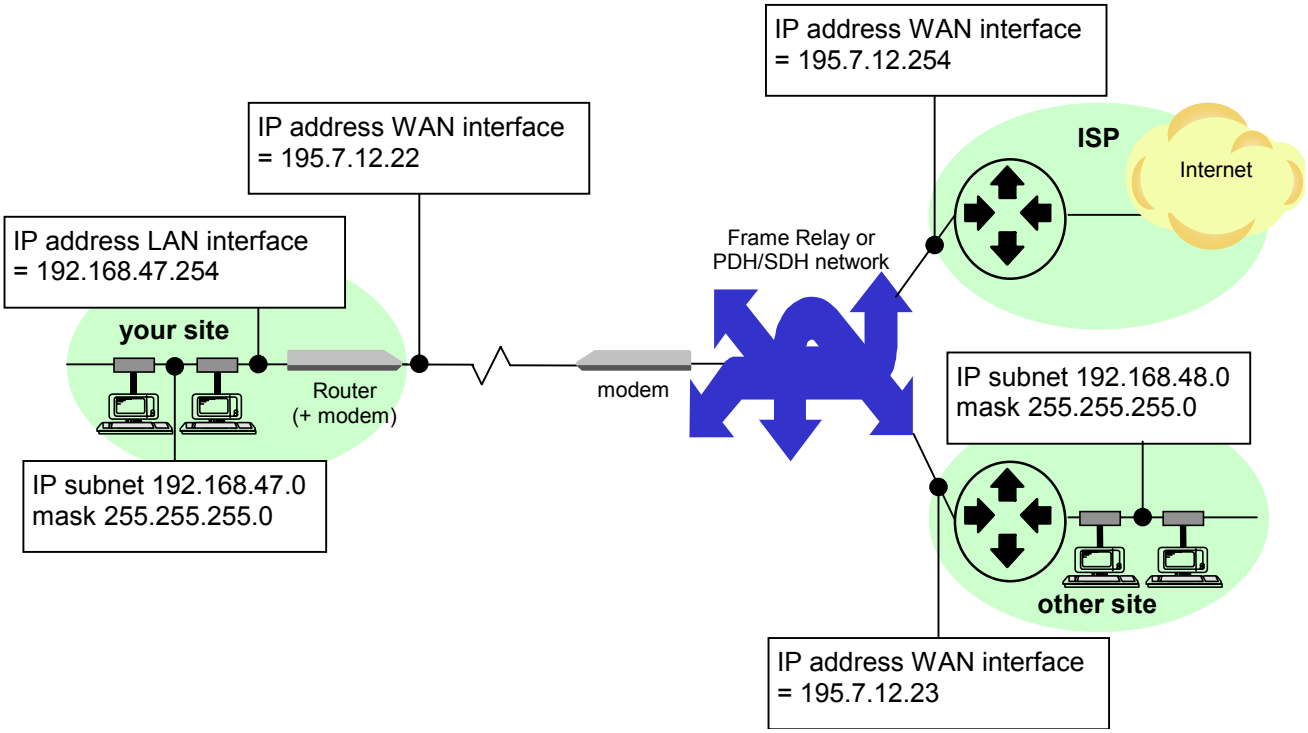
Suppose your network is connected to the Internet via a Frame Relay network and to another site that does not have official IP addresses either.

Now you have to choose whether to apply PAT to:

- all traffic towards the Frame Relay network

or

- the traffic destined for the Internet only.



Suppose PAT is only used for the traffic destined for the Internet. In that case, the configuration of the most relevant attributes of the Telindus 1031 Router is as follows:

- telindus1031/router/defaultRoute = { gateway = 195.7.12.254; interface = wan }
- telindus1031/router/routingTable = { network = 192.168.48.0; gateway = 195.7.12.23 }
- telindus1031/router/defaultNat/patAddress = 195.7.12.22

As you can see, the gateway attribute is not configured since the Internet traffic uses the default route.

Limitations

As seen from the previous, Port Address Translation has some limitations:

- Only outgoing sessions are supported. This implies that you can not access servers on your local network over the Internet.
- Some TCP or UDP applications do not support port translation.
- Limited ICMP support.

7.4.6 PAT limitations workaround

Use the following to partly overcome the PAT limitations:

- Use the portTranslations attribute to define specific port number ranges that should not be translated. Refer to telindus1031/router/defaultNat/portTranslations on page 215.
- Use the servicesAvailable attribute to define specific port number ranges for incoming Internet traffic that should not be translated. Instead it is sent to the corresponding private IP address. Refer to telindus1031/router/defaultNat/servicesAvailable on page 216.

Example of a portTranslations table

TMA is an example of an application that does not support port translation. If you want to make TMA connections from your local network to the outside world, you have to list TMA port number 1728 in this table. However, keep in mind that even then it is still not possible to have two simultaneous TMA sessions to the same outside world address.

portTranslations

	protocol	startPort	endPort	action
1	udp	1728	<Opt>	no translation
2	udp	2000	3000	deny

If you do not want that UDP packets with port numbers in the range 2000 up to 3000 are sent to the outside world, then you also have to include those in the table.

Example of a servicesAvailable table

In this example, a web server with address 192.168.47.250 on the local network is accessible from the Internet using the PAT address instead of using the server address.

servicesAvailable

	protocol	startPort	endPort	serverAddress
1	tcp	80	<Opt>	192.168.47.250

7.4.7 Configuring NAT

Despite the workarounds offered by the previous two PAT configuration attributes to overcome the limitations of PAT, there are situations where PAT is inadequate. For example, it is not possible to have several web servers on your local network. It is also impossible to run an application with fixed source port numbers on several local devices that are connected simultaneously to a single Internet device. This can only be solved by using several official IP addresses: Network Address Translation.

Use the following to configure NAT:

- Use the addresses attribute to enter all the official IP addresses that have to be used for Network Address Translation. Refer to telindus1031/router/defaultNat/addresses on page 216.
- Use the gateway attribute to define the gateway addresses from routes on which NAT or PAT should be applied. Refer to telindus1031/router/defaultNat/gateway on page 216.

Important remark - using NAT on the LAN interface

Consider the following configuration:

- telindus1031/lanInterface/ip/address = 172.31.74.1
- telindus1031/router/defaultNat/addresses = { officialAddress = 172.31.74.1; privateAddress = <opt> }
- telindus1031/wanInterface/ppp/ip/address = 2.2.2.2

The above means that NAT is used on the LAN interface and the router uses the address 172.31.74.1 as official IP address.

The problem that arises here is that the router can no longer be managed via the LAN interface using the management tool (TMA, Telnet, etc.). This because the NAT route has priority over the LAN route and, because it is a NAT address, the router does not accept incoming traffic on the address 172.31.74.1.

The solution is to add the WAN IP address to the addresses table as private address: telindus1031/router/addresses = { officialAddress = 172.31.74.1; privateAddress = 2.2.2.2 }. In that case, the management tool “service” runs on the WAN IP address. This means however, that the WAN has to be up.

7.4.8 How does the NAT address table work?

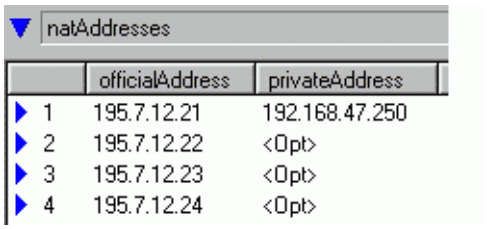
If a local station sends data to the Internet for the first time, NAT looks for an unused official IP address. It assigns this official IP address to the local station. The amount of local stations that can have simultaneous Internet access equals the amount of NAT addresses you defined. If all sessions between a local station and the Internet have been closed by the application (in case of TCP) or because of time-outs, then the previously assigned official IP address is freed for another local station.

Optionally, the NAT address entry may contain a corresponding private IP address. This allows to permanently assign an official IP address to a local station. This is useful for stations or servers that should have Internet access at all times. Another example of permanently assigned official IP addresses is a network where only a limited number of users has Internet access.

NAT only converts IP addresses and thus allows traffic in both directions. However, incoming traffic on one of the official IP addresses can only be forwarded to the local network if a corresponding private IP address has been configured.

Example of a NAT address table

In this example, the first address is continuously assigned to a server with IP address 192.168.47.250. The others are assigned dynamically.



7.4.9 Combining PAT and NAT

It is possible to use a combination of PAT and NAT. In that case the router first assigns NAT addresses until they are all used. Then it uses PAT addresses for further translations.

Make sure the PAT address does not appear in the NAT address table.

7.5 Configuring L2TP tunnelling

This section introduces the Layer 2 Tunnelling Protocol (L2TP) and gives a short description of the attributes you can use to configure L2TP.

The following gives an overview of this section:

- 7.5.1 - Introducing L2TP on page 128
- 7.5.2 - How does L2TP work? on page 129
- 7.5.3 - Configuring L2TP on page 129

7.5.1 Introducing L2TP

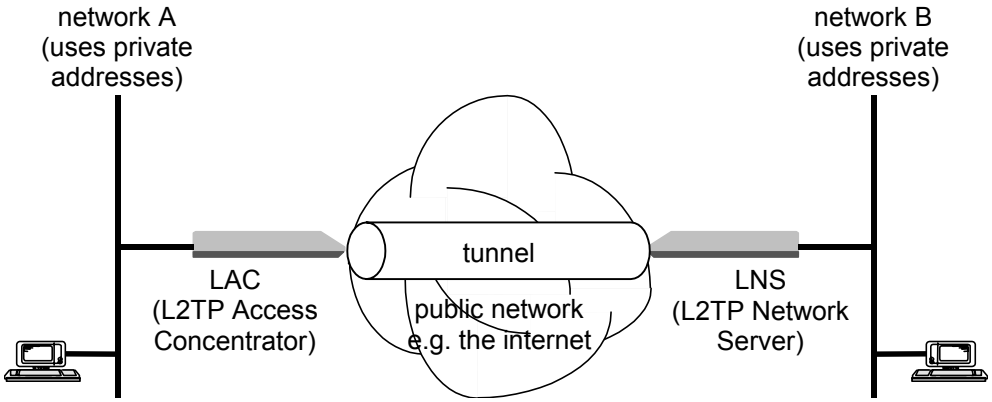
What is L2TP?

The Layer 2 Tunnelling Protocol (L2TP) is a protocol used for connecting VPNs (Virtual Private Networks) over public lines. More specific, it allows you to set up virtual PPP connections. In other words, an L2TP tunnel simulates an additional PPP interface which directly connects two routers with each other.

Concrete, using the Layer 2 Tunnelling Protocol you can connect several private and physically dispersed local networks with each other over public lines (such as the Internet) in order to create one big (virtual) local network. This without the need for address translation.

Example

In the following example, network A is virtually connected to network B through a tunnel in the public network:



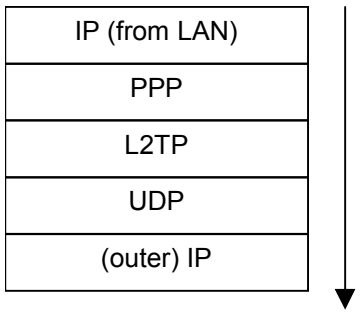
L2TP terminology

The following table gives some specific L2TP terminology:

Term	Description
L2TP Access Concentrator (LAC)	A node that acts as one side of an L2TP tunnel. It is a peer to the L2TP Network Server (LNS). Packets sent from the LAC to the LNS require tunnelling with the L2TP protocol.
L2TP Network Server (LNS)	A node that acts as one side of an L2TP tunnel. It is a peer to the L2TP Access Concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunnelled from the remote system by the LAC.
Tunnel	A tunnel exists between a LAC-LNS pair. The tunnel consists of a Control Connection and zero or more L2TP sessions. The tunnel carries encapsulated PPP datagrams and Control Messages between the LAC and the LNS.
Control Connection	A control connection operates in-band over a tunnel to control the establishment, release, and maintenance of sessions and of the tunnel itself.
Control Messages	Control messages are exchanged between LAC and LNS pairs, operating in-band within the tunnel protocol. Control messages govern aspects of the tunnel and sessions within the tunnel.

7.5.2 How does L2TP work?

Suppose a packet coming from the LAN has a destination address for a network that is accessible through a tunnel. The following happens:

Phase	Description
1	The packet goes through the routing decision process. If the result of this decision is a route which uses the tunnel interface, then the packet is encapsulated in PPP first, then L2TP, UDP and finally IP. 
2	Then the packet goes through the routing decision process again. This time using the outer IP header.
3	The packet is routed over the Internet using the outer IP header.
4	The packet is received in the tunnel's end point, where it is then routed again using the original IP header.

7.5.3 Configuring L2TP

Use the l2tpTunnels attribute to set up and configure an L2TP tunnel. Refer to telindus1031/router/tunnels/l2tpTunnels on page 218.

7.6 Configuring traffic and priority policy on the router

This section introduces traffic and priority policy and gives a short description of the attributes you can use to configure these features on the router. It also shows you the difference with the traffic policy on the bridge.

The following gives an overview of this section:

- 7.6.1 - Introducing traffic and priority policy on page 131
- 7.6.2 - Traffic and priority policy on routed and bridged data on page 132
- 7.6.3 - How to configure a traffic and priority policy on the router? on page 133
- 7.6.4 - Configuring a traffic policy on the router on page 134
- 7.6.5 - Configuring a priority policy on page 135
- 7.6.6 - Applying a routing traffic policy on a certain interface on page 136
- 7.6.7 - Applying a priority policy on a certain interface on page 137

7.6.1 Introducing traffic and priority policy

What is traffic and priority policy?

Because of the bursty nature of voice / video / data traffic, sometimes the amount of traffic exceeds the speed of a link. At this point, the Telindus 1031 Router has to decide what to do with this “excess” of traffic:

- Buffer the traffic in a single queue and let the first packet in be the first packet out?
- Or put packets into different queues and service certain queues more often (also known as priority queuing)?

These questions are dealt with by the traffic and priority policy mechanisms:

- The traffic policy determines, on traffic overload conditions, how and which queues are filled with the “excess” data.
- The priority policy determines how and which queues are emptied.

What is a priority queuing?

Using the traffic and priority policy features you can perform priority queuing. This allows you to define how traffic is prioritised in the network. E.g. to ensure that voice, video or other streaming media is serviced before (or after) other traffic types, to ensure that web response traffic is routed before normal web browsing traffic, etc.

There are 7 queues:

Queue	Queue type	Description
1 - 5	user configurable queue	The user can decide which data goes into which queue.
6	low delay queue	The user can decide which data goes into this queue. This queue usually is addressed more often then the user configurable queues.
7	system queue	This queue is filled with mission critical data (e.g.link monitoring messages etc.) and has priority over all other queues.

7.6.2 Traffic and priority policy on routed and bridged data

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction.

The following table shows which traffic policy is used to fill the queues with routed data and which is used to fill the queues with bridged data:

In case … is enabled,	**then …**
only routing	the routed data is queued as specified in the traffic policy settings as defined in the telindus1031/router/trafficPolicy[ ] object.
routing and bridging	• the routed data is queued as specified in the traffic policy settings as defined in the telindus1031/router/trafficPolicy[ ] object. • the bridged data is queued as specified in the traffic policy settings as defined in the telindus1031/bridge/trafficPolicy[ ] object.
only bridging	the bridged data is queued as specified in the traffic policy settings as defined in the telindus1031/bridge/trafficPolicy[ ] object.

To empty the queues, the priority policy settings as defined in the telindus1031/router/priorityPolicy[ ] object are used for both routed and bridged data.

7.6.3 How to configure a traffic and priority policy on the router?

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction.

The following table explains you step-by-step how to configure a traffic and priority policy on the router. To configure a traffic and priority policy for the routed data of a certain interface, proceed as follows:

Step	Action
1	Add a trafficPolicy object under the router object and give it a certain index name (e.g. trafficPolicy[my_traffic_policy]). Refer to 4.4 - Adding an object to the containment tree on page 45.
2	Configure the traffic policy related parameters. Refer to 7.6.4 - Configuring a traffic policy on the router on page 134.
3	Add a priorityPolicy object under the router object and give it a certain index name (e.g. priorityPolicy[my_priority_policy]). Refer to 4.4 - Adding an object to the containment tree on page 45.
4	Configure the priority policy related parameters. Refer to 7.6.5 - Configuring a priority policy on page 135.
5	Apply the traffic policy to a certain interface. Do this by typing the index name of the added trafficPolicy object in the appropriate element. Refer to 7.6.6 - Applying a routing traffic policy on a certain interface on page 136.
6	Apply the priority policy to a certain interface. Do this by typing the index name of the added priorityPolicy object in the appropriate element. Refer to 7.6.7 - Applying a priority policy on a certain interface on page 137.

7.6.4 Configuring a traffic policy on the router

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction.

This section shows you which configuration attributes you can use to configure a traffic policy on the router.

The trafficPolicy object is not present in the containment tree by default. If you want to use traffic policy, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.

First you have to choose a method you want to use to fill the queues when a traffic overload condition occurs. Do this using the attribute telindus1031/router/trafficPolicy[ ]/method on page 223.

Once you choose a traffic policy method, you can fine-tune this method using the following attributes:

If you choose the method …	then use the following attribute to fine-tune this method:
trafficShaping,	• telindus1031/router/trafficPolicy[ ]/trafficShaping on page 224. • telindus1031/router/trafficPolicy[ ]/dropLevels on page 226 (only the maxLength1 element).
tosDiffServ,	telindus1031/router/trafficPolicy[ ]/dropLevels on page 226.
tosMapped,	• telindus1031/router/trafficPolicy[ ]/tos2QueueMapping on page 227. • telindus1031/router/trafficPolicy[ ]/dropLevels on page 226 (only the maxLength1 element).

7.6.5 Configuring a priority policy

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction.

This section shows you which configuration attributes you can use to configure a priority policy.

- The priorityPolicy object is not present in the containment tree by default. If you want to use priority policy, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.
- Whereas configuring a traffic policy for routed data is different than for bridged data, configuring a priority policy is the same for both. In other words, the mechanism to fill the queues is different for routed data than it is for bridged data, but the mechanism to empty the queues is the same for both routed and bridged data.

First you have to choose an algorithm you want to use to empty the queues. Do this using the attribute telindus1031/router/priorityPolicy[ ]/algorithm on page 228.

Then you can define the number of bytes/packets that has to be dequeued from the user configurable queues when these queues are addressed. Do this using the attribute telindus1031/router/priorityPolicy[ ]/queueConfigurations on page 230. Also with this attribute you can set the relative importance of the user configurable queues (this is only relevant in case the telindus1031/router/priorityPolicy[ ]/algorithm attribute is set to weightedFairQueueing).

7.6.6 Applying a routing traffic policy on a certain interface

This section shows you where to find the appropriate traffic policy elements in order to apply a traffic policy on a certain interface[1].

The following table shows you in which trafficPolicy element you have to enter the index name of the earlier created trafficPolicy object in order to apply a traffic policy on the routed data of a certain interface:

<table>
<tr><th>For the …</th><th>you can find the trafficPolicy element in …</th></tr>
<tr><td>LAN interface,</td><td>the ip structure under the lanInterface object: telindus1031/lanInterface/ip.

Important remark

On the LAN interface, you can not apply a traffic policy with the purpose of queueing. On this interface, the traffic policy is intended to serve as extended access list. Refer to 7.7 - Configuring an extended access list on page 138.</td></tr>
<tr><td>WAN interface,</td><td>each WAN encapsulation object:

<table>
<tr><td>frameRelay</td><td>You can find the trafficPolicy element in the ip structure within the dlciTable attribute under the frameRelay object: telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/ip/trafficPolicy.

This means that you can specify a traffic policy per DLCI.</td></tr>
<tr><td>ppp</td><td>You can find the trafficPolicy element in the ip structure under the ppp object: telindus1031/g703[ ]/channel[ ]/ppp/ip/trafficPolicy.</td></tr>
<tr><td>atm</td><td>You can find the trafficPolicy element in the ip structure within the pvcTable attribute under the atm object: telindus1031/g703[ ]/channel[ ]/atm/pvcTable/ip/trafficPolicy.

This means that you can specify a traffic policy per PVC.</td></tr>
</table>
</td></tr>
<tr><td>tunnels,</td><td>in the ip structure within the l2tpTunnels attribute under the tunnels object: telindus1031/router/tunnels/l2tpTunnels/ip/trafficPolicy.</td></tr>
<tr><td>bridge,</td><td>in the ip structure under the bridgeGroup object: telindus1031/bridge/bridgeGroup/ip.</td></tr>
</table>

1. The interface can be a physical interface (such as the LAN interface), but can also be a DLCI, a PVC, a tunnel, etc.

7.6.7 Applying a priority policy on a certain interface

This section shows you where to find the appropriate priority policy attribute in order to apply a priority policy on a certain interface[1].

The priorityPolicy attribute can be found under the wanInterface object: telindus1031/g703[ ]/channel[ ]/priorityPolicy.

This implies that in case of Frame Relay, you can not specify a priority policy per DLCI. In case of ATM, however, you can specify a priority policy per PVC. To do so, use the priorityPolicy element in the pvcTable under the ATM object: telindus1031/g703[ ]/channel[ ]/atm/pvcTable/priorityPolicy.

1. The interface can be a physical interface (such as the LAN interface), but can also be a DLCI, a PVC, a tunnel, etc.

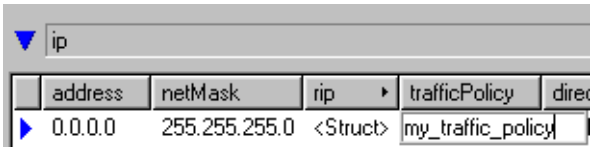
7.7 Configuring an extended access list

In case you set the telindus1031/router/trafficPolicy[ ]/method attribute to trafficShaping (default value), then you can use the telindus1031/router/trafficPolicy[ ]/trafficShaping attribute to set up an extended access list.

The extended access list itself is activated by specifying the trafficPolicy object its index name in a trafficPolicy element of a certain interface.

Example

Suppose you want to set up an extended access list on the LAN interface. Then proceed as follows:

Step	Action
1	Add a trafficPolicy object to the containment tree. Refer to 4.4 - Adding an object to the containment tree on page 45. Suppose you name it my_traffic_policy.
2	Go to the ip attribute in the lanInterface object.
3	In the ip attribute, enter the index name of the added trafficPolicy object as value of the trafficPolicy element. In this case: my_traffic_policy. 
4	Set the configuration attribute telindus1031/router/trafficPolicy[ ]/method to trafficShaping.
5	Configure the configuration attribute telindus1031/router/trafficPolicy[ ]/trafficShaping to your needs.

8 Configuring the bridge

This chapter introduces bridging on the Telindus 1031 Router and lists the attributes you can use to configure bridging.

The following gives an overview of this chapter:

- 8.1 - Introducing bridging on page 140
- 8.2 - The self-learning and Transparent Spanning Tree bridge on page 141
- 8.3 - The Spanning Tree root bridge on page 142
- 8.4 - The Spanning Tree topology on page 143
- 8.5 - The Spanning Tree bridge port states on page 144
- 8.6 - The Spanning Tree Bridge Protocol Data Unit on page 145
- 8.7 - The Spanning Tree behaviour on page 146
- 8.8 - The Spanning Tree priority and cost on page 147
- 8.9 - Configuring bridging on page 149
- 8.10 - Configuring traffic and priority policy on the bridge on page 154

Refer to the Reference manual on page 169 for a complete overview of the attributes of the Telindus 1031 Router.

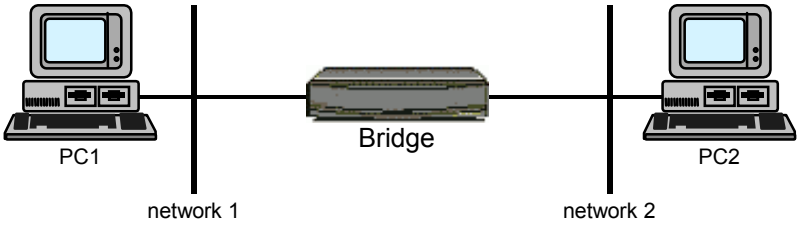
8.1 Introducing bridging

What is bridging?

The Telindus 1031 Router can be configured to act as a bridge. This enables you to split up your LAN network into smaller parts or segments. This decreases the amount of data traffic on the separated LAN segments and, consequently, increases the amount of available bandwidth.

Example

The following figure shows an example of bridging:



Data coming from network 1, will only be let through by the bridge if this data has a destination outside network 1 or if it has a broadcast or multicast address. This means the bridge filters the data and decreases the amount of data traffic on the separated LAN segments.

8.2 The self-learning and Transparent Spanning Tree bridge

The Telindus 1031 Router features two bridging mechanisms:

- self-learning bridging,
- self-learning bridging in conjunction with the Transparent Spanning Tree (TST) algorithm, or briefly Spanning Tree bridging.

Bridging principle	Description
self-learning	The bridge learns which data it has to forward to the other LAN segment and which data it has to block. I.e. it builds its own bridging table. In other words, you do not have to configure a bridging table with MAC addresses of stations that are located on the separated LAN segments but that have to be able to communicate with each other.
self-learning + TST	This is based on the self-learning principle, but a protocol is used to implement the TST algorithm. **Bridging loops** The primary goal of this algorithm is to avoid that bridging loops arise. A bridging loop occurs when two self-learning bridges are placed in parallel. This results in data that keeps circling around as each bridge forwards the same data. **The TST algorithm** Using the TST algorithm, bridges know of each others existence. By communicating with each other, they establish one single path for reaching any particular network segment. If necessary, they may decide to disable some bridges in the network in order to establish this single path. This is a continuous process. So if a bridge fails, the remaining bridges will reconfigure their bridging tables keeping each LAN segment reachable.

8.3 The Spanning Tree root bridge

What is the root bridge?

Spanning Tree defines a tree with a root bridge and a loop-free path from the root to all bridges in the extended network. The root bridge is the logical centre of the Spanning Tree topology.

Redundant data paths are forced into a stand-by (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the stand-by path.

How is a root bridge selected?

All bridges in the network participating in Spanning Tree gather information about other bridges in the network. They do this through an exchange of data messages called Bridge Protocol Data Units (BPDUs).

This exchange of messages results in the following phases:

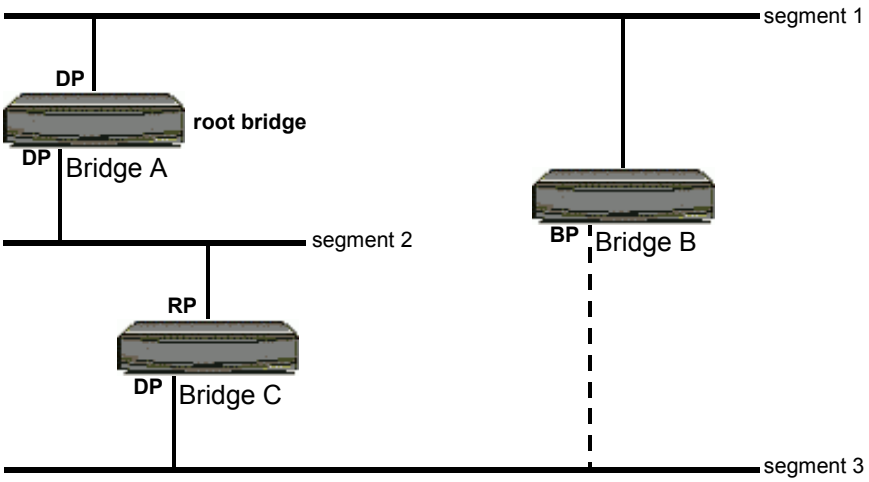
Phase	Description
1	The selection of a root bridge. The bridge with the highest bridge priority (i.e. the lowest numerical priority value) is selected as the root bridge. If all bridges are configured with the default priority (32768), the bridge with the lowest MAC address becomes the root bridge.
2	The selection of a designated bridge for every bridged LAN segment.
3	The removal of loops in the bridged network by blocking bridge ports connected to redundant links.

8.4 The Spanning Tree topology

The cost factor is used to calculate the distance from each port of a bridge to the root bridge. On the basis of this, each port on a bridge is assigned one of the following states:

State	Description
root port	The port that is closest to the root bridge. Only one port on each bridge is assigned as the root port.
designated port	The port that connects to bridges further away from the root bridge. The root bridge only has designated ports.
blocking	If a port is not assigned a root port or a designated port state, they are assigned a blocking state. Frames (with the exception of Configuration BPDUs) are not accepted or transmitted by the port when it is in the blocking state. The port can be said to be in stand-by.

An elementary example of a Spanning Tree topology is given in the figure below:



RP = Root Port
DP = Designated Port
BP = Blocking Port

8.5 The Spanning Tree bridge port states

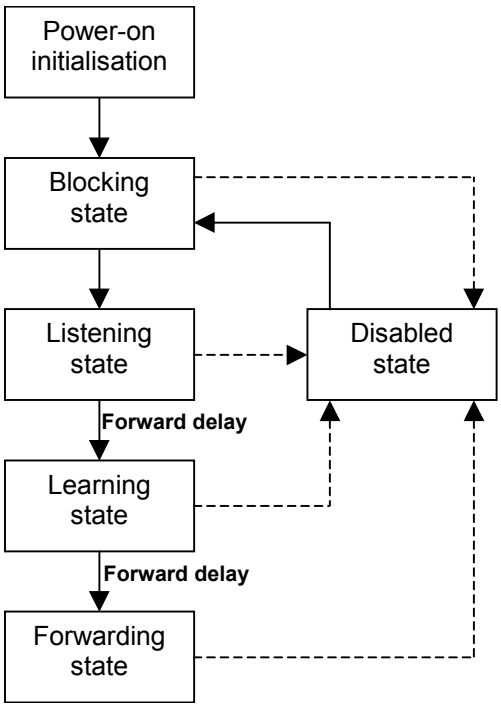
Bridge port states

There are four possible states a bridge port can be in:

State	A port in this state …
blocking	• does no frame forwarding. • does not incorporate station location into its address database (There is no learning on a blocking port, so there is no MAC address database update.). • receives BPDUs, but does not process or propagate them. A bridge always enters the blocking state following bridge initialisation.
listening	• does no frame forwarding. • does not incorporate station location into its address database (There is no learning on a listening port, so there is no MAC address database update.). • receives and processes BPDUs, but does not propagate them.
learning	• does no frame forwarding. • incorporates station location into its MAC address database. • receives, processes and propagates BPDUs.
forwarding	• forwards frames. • incorporates station location into its MAC address database. • receives, processes and propagates BPDUs.

Bridge port state transition diagram

The following figure shows how a bridge port moves through the different states when the bridge is powered:



When you enable Spanning Tree, every bridge in the network goes through the transitory states of listening and learning at power up. If properly configured, each port stabilises to the forwarding or blocking state.

When the spanning-tree algorithm places a port in the forwarding state, the following process occurs:

1. The port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.
2. The port waits for the expiration of the forward delay timer, moves the port to the learning state, and resets the forward delay timer.
3. In the learning state, the port continues to block frame forwarding as it learns station location information for the forwarding database.
4. The port waits for the expiration of the forward delay timer and then moves the port to the forwarding state, where both learning and forwarding are enabled.

8.6 The Spanning Tree Bridge Protocol Data Unit

What is a BPDU?

To establish a stable path, each bridge sends Configuration Bridge Protocol Data Units (BPDUs) to its neighbouring bridges. These Configuration BPDU messages contain information about the spanning tree topology. The contents of these frames only changes when the bridged network topology changes or has not been established.

Each Configuration BPDU contains the following minimal information:

- The unique bridge identifier of the bridge that the transmitting bridge believes to be the root bridge.
- The cost of the path to the root from the transmitting port.
- The unique port identifier of the transmitting port.

When a bridge transmits a BPDU frame, all bridges connected to the LAN on which the frame is transmitted receive the BPDU. When a bridge receives a BPDU, it does not forward the frame. Instead, it uses the information in the frame to:

- calculate a BPDU,
- initiate a BPDU transmission if the topology changes.

The propagation of Configuration BDPUs

When a bridged network is in a stable condition, switches continue to send Configuration BPDUs to its neighbouring bridges at regular intervals. Configuration BPDUs are transmitted down the spanning tree from designated ports to root ports. If a Configuration BPDU is not received by the root port of a bridge within a predefined time interval (for example, because a bridge along the path has dropped out), the port enters the listening state to re-determine a stable path.

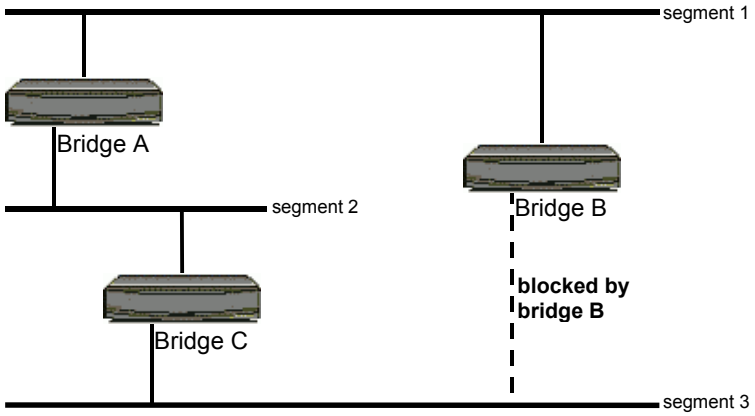
8.7 The Spanning Tree behaviour

The following are some examples of how Spanning Tree behaves when certain events occur in your network.

Bridging loops

Bridges connected in a LAN must detect potential bridge loops. They must then remove these loops by blocking the appropriate ports to other bridges.

This is illustrated in the following figure:

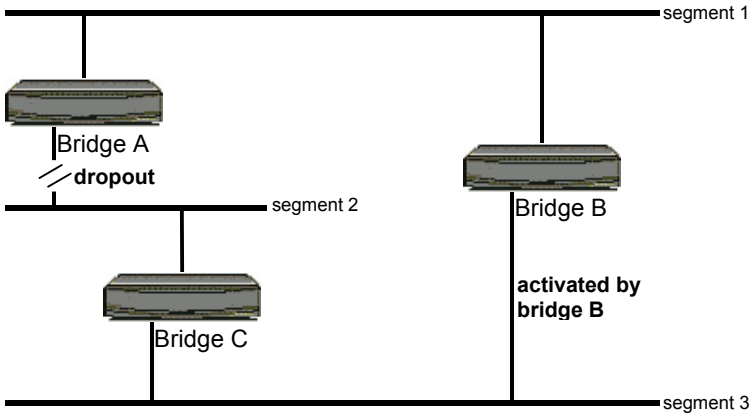


An alternate path has been established by connecting Bridge B in parallel with Bridges A and C. This also creates a potential bridge loop. However, by using the Spanning Tree Algorithm, Bridge B breaks the loop and blocks its path to segment 3.

Bridge failure

Bridges connected in a LAN must also detect bridge failure. They must then establish an alternative path. Should the root bridge fail, also a new root bridge must be selected.

A bridge failure is illustrated in the following figure:

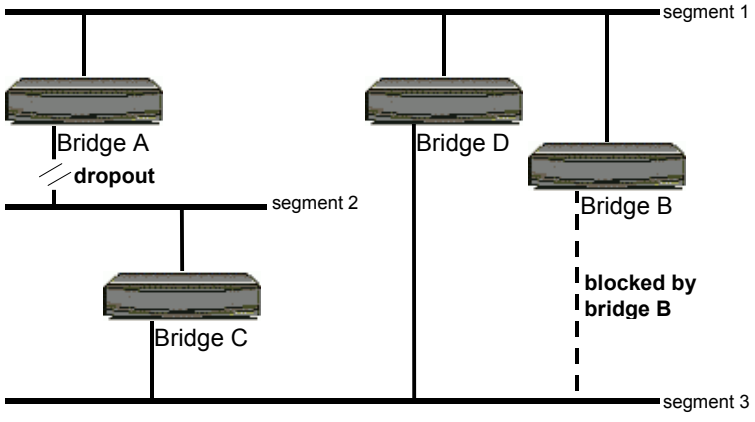


If Bridge A fails, the Spanning Tree Algorithm must be capable of activating an alternative path, such as Bridge B.

Network extension

Bridges connected in a LAN must also detect topology changes. They must adapt to these changes.

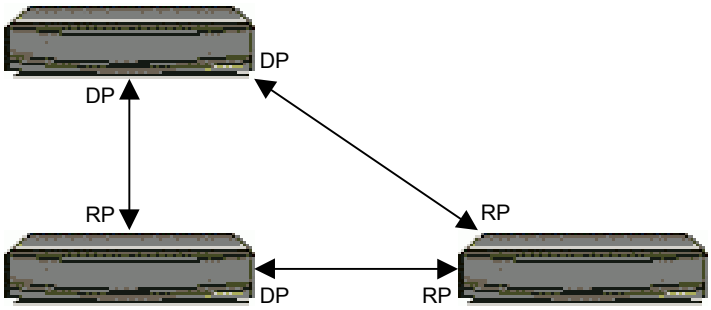
A topology change is illustrated in the following figure:



If the network is extended by adding Bridge D, the Spanning Tree Algorithm must be capable of adapting automatically to the new topology. This means that Bridge B stops looping by blocking the path to segment 3.

8.8 The Spanning Tree priority and cost

Consider the following Spanning Tree Topology:



RP = Root Port
DP = Designated Port

What is bridge priority?

In the example above, Bridge A is selected as the root bridge. This because the bridge priority of all the bridges is set to the default value (32768) and Bridge A has the lowest MAC address. However, due to traffic patterns or link types, Bridge A might not be the ideal root bridge.

By increasing the bridge priority (lowering the numerical priority value) of the ideal bridge so that it becomes the root bridge, you force a Spanning Tree recalculation to form a new spanning-tree topology with the ideal bridge as the root.

What is port priority and path cost?

When the spanning-tree topology is calculated based on default parameters, the path between source and destination stations in a bridged network might not be ideal. The goal is to make the fastest link the root port.

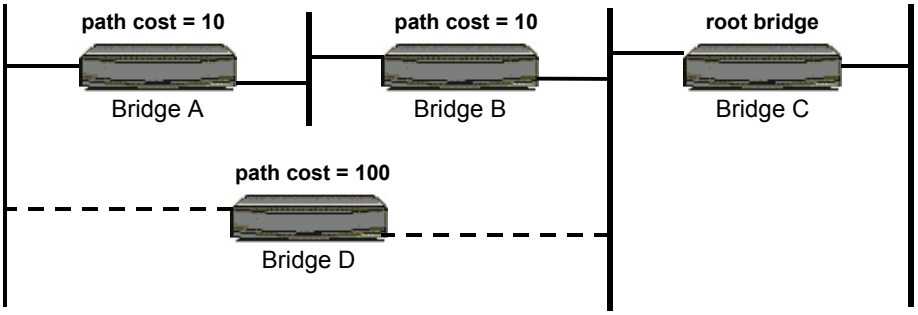
For example, assume on Bridge B that …

- port 1, currently the root port, is an unshielded twisted-pair link,
- port 2 is a fibre-optic link.

Network traffic might be more efficient over the high-speed fibre-optic link. By changing the spanning-tree port priority or path cost for port 2 to a higher priority (lower numerical value) than port 1, port 2 becomes the root port.

Example

By changing the priority and/or the pathCost, you can create a "preferred" path:



By setting the path costs of Bridge A and B to a lower value than the path cost of Bridge D, you can create a *preferred* path through Bridge A and B. The path through Bridge D becomes the *back-up* path.

8.9 Configuring bridging

This section lists the attributes you can use to configure bridging. The following gives an overview of this section:

- 8.9.1 - Configuring an IP address on page 150
- 8.9.2 - Enabling bridging on the interfaces on page 150
- 8.9.3 - Selecting the bridging protocol on page 150
- 8.9.4 - Setting the bridge priority on page 150
- 8.9.5 - Configuring the bridging parameters on the interfaces on page 151
- 8.9.6 - Explaining the bridging structure on page 152

8.9.1 Configuring an IP address

If you enable bridging on the LAN interface (telindus1031/lanInterface/mode = bridging), then the settings of the configuration attribute telindus1031/lanInterface/ip are ignored. As a result, if you want to manage the Telindus 1031 Router via IP, you have to configure an IP address in the bridgeGroup object instead: telindus1031/bridge/bridgeGroup/ip.

8.9.2 Enabling bridging on the interfaces

Refer to 8.1 - Introducing bridging on page 140 for an introduction on bridging.

Use the mode attribute to enable or disable bridging per interface. The location of this attribute depends on the interface:

Interface	Location of the mode attribute
LAN	telindus1031/lanInterface/mode on page 180
WAN - Frame Relay	telindus1031/wanInterface/frameRelay/dlciTable/mode on page 189
WAN - PPP	telindus1031/g703[ ]/channel[ ]/ppp/mode on page 185
WAN - ATM	telindus1031/wanInterface/atm/pvcTable/mode on page 193
tunnel	telindus1031/router/tunnels/l2tpTunnels/mode on page 218

8.9.3 Selecting the bridging protocol

Refer to 8.2 - The self-learning and Transparent Spanning Tree bridge on page 141 for an introduction.

Use the protocol element in the spanningTree structure to select the bridging protocol. Refer to telindus1031/bridge/bridgeGroup/spanningTree on page 234.

8.9.4 Setting the bridge priority

Refer to 8.8 - The Spanning Tree priority and cost on page 147 for more information on bridge priority.

Use the bridgePriority element in the spanningTree structure to set the bridge priority. Refer to telindus1031/bridge/bridgeGroup/spanningTree on page 234.

8.9.5 Configuring the bridging parameters on the interfaces

Use the bridging structure to configure the bridging parameters per interface. The location of this structure depends on the interface:

Interface	Location of the bridging attribute
LAN	telindus1031/lanInterface/bridging
WAN - Frame Relay	telindus1031/wanInterface/frameRelay/dlciTable/bridging
WAN - PPP	telindus1031/g703[ ]/channel[ ]/ppp/bridging
WAN - ATM	telindus1031/wanInterface/atm/pvcTable/bridging
tunnel	telindus1031/router/tunnels/l2tpTunnels/bridging

Refer to 8.9.6 - Explaining the bridging structure on page 152 for a detailed explanation of the bridging structure.

8.9.6 Explaining the bridging structure

Because the bridging structure occurs in several objects, it is described here once and referenced where necessary. Refer to 8.9.5 - Configuring the bridging parameters on the interfaces on page 151 for the location of the bridging structure.

This section lists all the elements that can be present in the bridging structure. However, depending on the interface, it is possible that not all of these elements are present.

The bridging structure contains the following elements:

Element	Description
accessList	Use this element set up an access list on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the access list you want to use. You can create the access list itself by adding an accessList object under the bridge object and by configuring the attributes in this object. **Example** If you created a accessList object with index name my_access_list (i.e. accessList[my_access_list]) and you want to apply this access list here, then enter the index name as value for the accessList element. Refer to … • 10.6.2 - Bridge access list configuration attributes on page 236 for more information on access lists. • 4.4 - Adding an object to the containment tree on page 45 for more information on adding objects.

Element	Description
trafficPolicy	This element is not present in the telindus1031/lanInterface/bridging structure. Use this element to apply a traffic policy on the bridged data on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the traffic policy you want to use. You can create the traffic policy itself by adding a trafficPolicy object under the bridge object and by configuring the attributes in this object. **Example** If you created a trafficPolicy object with index name my_traffic_policy (i.e. trafficPolicy[my_traffic_policy]) and you want to apply this traffic policy here, then enter the index name as value for the trafficPolicy element. Refer to … • 8.10 - Configuring traffic and priority policy on the bridge on page 154 for more information on policies. • 4.4 - Adding an object to the containment tree on page 45 for more information on adding objects.
priority	Use this element to set the port priority of the interface. Default:128 Range: 0 … 255 Each port of a bridge has a *unique port identifier*. The priority element is a part of this port identifier and allows you to change the priority of the port. It is taken as the more significant part in priority comparisons. The other part of the unique port identifier has a fixed relationship to the physical or logical port. This assures the uniqueness of the unique port identifier among the ports of a single bridge. Refer to 8.8 - The Spanning Tree priority and cost on page 147 for more information on port priority.
pathCost	Use this element to set the path cost of the interface. Default:100 Range: 1 … 65535 The path cost is the value that is added to the total cost of the path to the root bridge, provided that this particular port is a root port. I.e. that the path to the root goes through this port. The total cost of the path to the root bridge should not exceed 65500. Refer to 8.8 - The Spanning Tree priority and cost on page 147 for more information on port priority.
topologyChange-Detection	Use this element to enable or disable the communication of Spanning Tree topology changes to the root bridge. Default:enabled Range: enabled / disabled

8.10 Configuring traffic and priority policy on the bridge

This section introduces traffic and priority policy and gives a short description of the attributes you can use to configure these features on the bridge.

The following gives an overview of this section:

- 8.10.1 - How to configure a traffic and priority policy on the bridge? on page 155
- 8.10.2 - Configuring a traffic policy on the bridge on page 156
- 8.10.3 - Applying a bridging traffic policy on a certain interface on page 157

Refer to …

- 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction on traffic and priority policy.
- 7.6.2 - Traffic and priority policy on routed and bridged data on page 132 for the difference between traffic and priority policy on the bridge and the router.

8.10.1 How to configure a traffic and priority policy on the bridge?

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction.

The following table explains you step-by-step how to configure a traffic and priority policy on the bridge. To configure a traffic and priority policy for the bridged data of a certain interface, proceed as follows:

Step	Action
1	Add a trafficPolicy object under the bridge object and give it a certain index name (e.g. trafficPolicy[my_traffic_policy]). Refer to 4.4 - Adding an object to the containment tree on page 45.
2	Configure the traffic policy related parameters. Refer to 8.10.2 - Configuring a traffic policy on the bridge on page 156.
3	Add a priorityPolicy object under the router object and give it a certain index name (e.g. priorityPolicy[my_priority_policy]). Refer to 4.4 - Adding an object to the containment tree on page 45.
4	Configure the priority policy related parameters. Refer to 7.6.5 - Configuring a priority policy on page 135.
5	Apply the traffic policy to a certain interface. Do this by typing the index name of the added trafficPolicy object in the appropriate element. Refer to 8.10.3 - Applying a bridging traffic policy on a certain interface on page 157.
6	Apply the priority policy to a certain interface. Do this by typing the index name of the added priorityPolicy object in the appropriate element. Refer to 7.6.7 - Applying a priority policy on a certain interface on page 137.

8.10.2 Configuring a traffic policy on the bridge

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for an introduction.

This section shows you which configuration attributes you can use to configure a traffic policy on the bridge.

The trafficPolicy object is not present in the containment tree by default. If you want to use traffic policy, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.

You have to specify how the queues are filled when a traffic overload condition occurs. Do this using the attribute telindus1031/bridge/trafficPolicy/vlanPriorityMap on page 237.

Important remark

Whereas configuring a traffic policy for routed data is different than for bridged data, configuring a priority policy is the same for both. In other words, the mechanism to fill the queues is different for routed data than it is for bridged data, but the mechanism to empty the queues is the same for both routed and bridged data. Refer to 7.6.5 - Configuring a priority policy on page 135.

8.10.3 Applying a bridging traffic policy on a certain interface

This section shows you where to find the appropriate traffic policy elements in order to apply a traffic policy on a certain interface[1].

The following table shows you in which trafficPolicy element you have to enter the index name of the earlier created trafficPolicy object in order to apply a traffic policy on the bridged data of a certain interface:

<table>
<tr><th>For the …</th><th>you can find the trafficPolicy element in …</th></tr>
<tr><td>WAN interface,</td><td>each WAN encapsulation object:
<table>
<tr><td>frameRelay</td><td>You can find the trafficPolicy element in the bridging structure within the dlciTable attribute under the frameRelay object: telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/bridging/trafficPolicy.
This means that you can specify a traffic policy per DLCI.</td></tr>
<tr><td>ppp</td><td>You can find the trafficPolicy element in the bridging structure under the ppp object: telindus1031/g703[ ]/channel[ ]/ppp/bridging/trafficPolicy.</td></tr>
<tr><td>atm</td><td>You can find the trafficPolicy element in the bridging structure within the pvcTable attribute under the atm object: telindus1031/g703[ ]/channel[ ]/atm/pvcTable/bridging/trafficPolicy.
This means that you can specify a traffic policy per PVC.</td></tr>
</table></td></tr>
<tr><td>tunnels,</td><td>in the bridging structure within the l2tpTunnels attribute under the tunnels object: telindus1031/router/tunnels/l2tpTunnels/bridging/trafficPolicy.</td></tr>
</table>

You can not apply a bridging traffic policy on the LAN interface.

1. The interface can be a physical interface (such as the LAN interface), but can also be a DLCI, a PVC, a tunnel, etc.

9 Configuration examples

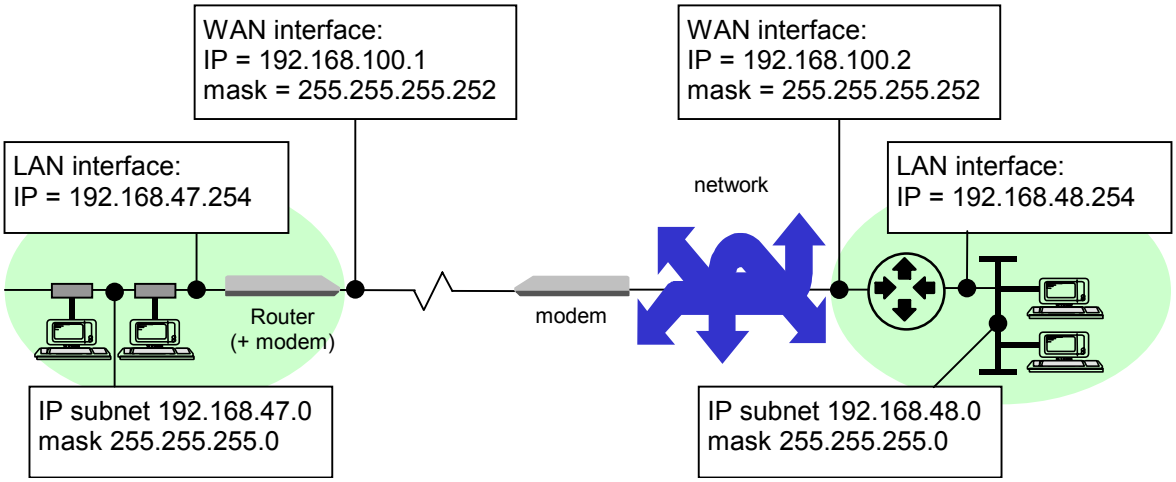
This chapter shows some configuration examples for the Telindus 1031 Router. The following gives an overview of this chapter:

- 9.1 - LAN extension over a PDH/SDH network on page 160
- 9.2 - LAN extension over a Frame Relay network on page 161
- 9.3 - LAN extension over an ATM network on page 162
- 9.4 - Connecting a LAN to the Internet using NAT and PAT on page 163
- 9.5 - Using PAT over PPP with a minimum of official IP addresses on page 164
- 9.6 - Combining bridging and routing in a network on page 165
- 9.7 - Connecting two networks through a tunnel on page 166
- 9.8 - Connecting VLAN enabled switches over a WAN on page 168

9.1 LAN extension over a PDH/SDH network

In this example, a remote office is connected to a central office over a PDH or SDH network.

A modem link connects the remote office to the PDH or SDH network. At the local office a Telindus 1031 Router is installed. The central router is a third party router. The WAN encapsulation is PPP with active link monitoring.



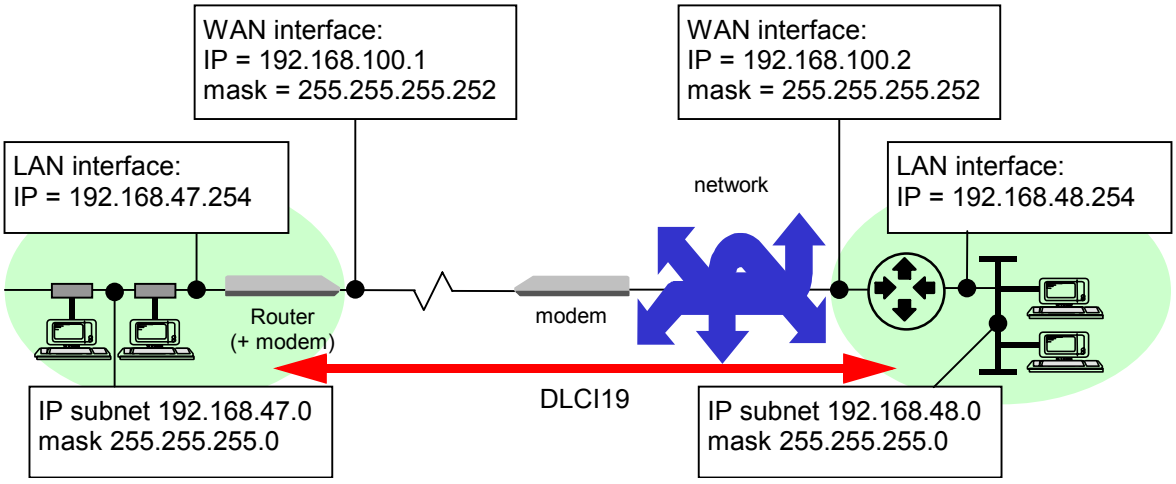
The configuration of the Telindus 1031 Router in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        address = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = ppp
      }
      SELECT ppp
      {
        LIST
        {
          ip =
          {
            address = 192.168.100.1
            netMask = 255.255.255.252
          }
          linkMonitoring =
          {
            operation = enabled
          }
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      routingTable =
      {
        [a] =
        {
          network = 192.168.48.0
          mask = 192.168.100.2
        }
      }
    }
  }
}
action "Activate Configuration"
```

9.2 LAN extension over a Frame Relay network

In this example, a remote office is connected to a central office over a Frame Relay network.

A modem link connects the remote office to the Frame Relay network. At the local office a Telindus 1031 Router is installed. The central router is a third party router.The Frame Relay network uses LMI according to the ANSI standard. No Reverse ARP is supported by the network.



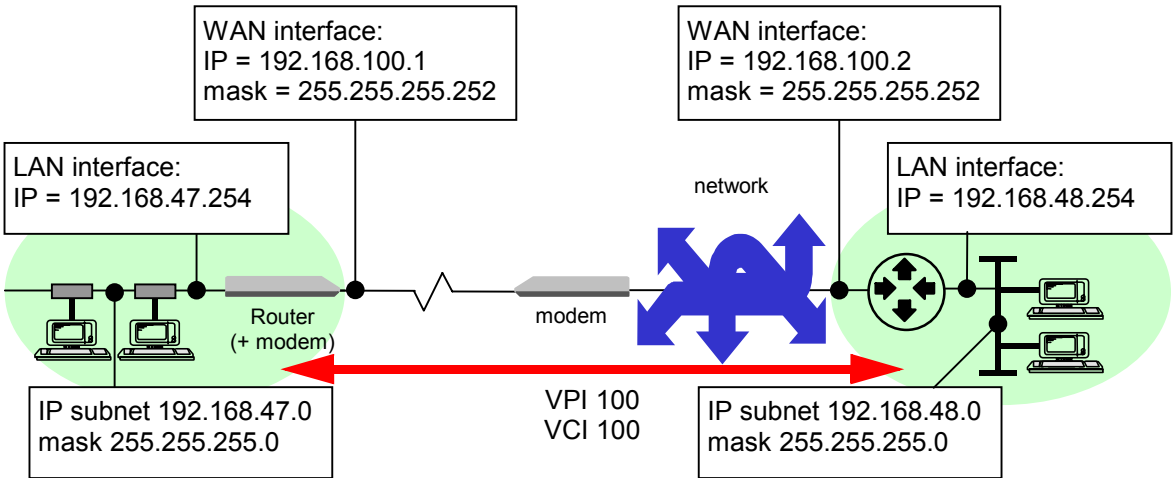
The configuration of the Telindus 1031 Router in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        address = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = frameRelay
      }
      SELECT frameRelay
      {
        LIST
        {
          dlciTable =
          {
            [a] =
            {
              name = dlci1
              ip =
              {
                address = 192.168.100.1
                netMask = 255.255.255.252
                remote = 192.168.100.2
              }
              frameRelay =
              {
                dlci = 19
              }
            }
          }
          lmi =
          {
            type = ansiT1-617-d
          }
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      routingTable =
      {
        [a] =
        {
          network = 192.168.48.0
          gateway = 192.168.100.2
        }
      }
    }
  }
}
action "Activate Configuration"
```

9.3 LAN extension over an ATM network

In this example, a remote office is connected to a central office over an ATM network.

A modem link connects the remote office to the ATM network. At the local office a Telindus 1031 Router is installed. The central router is a third party router.



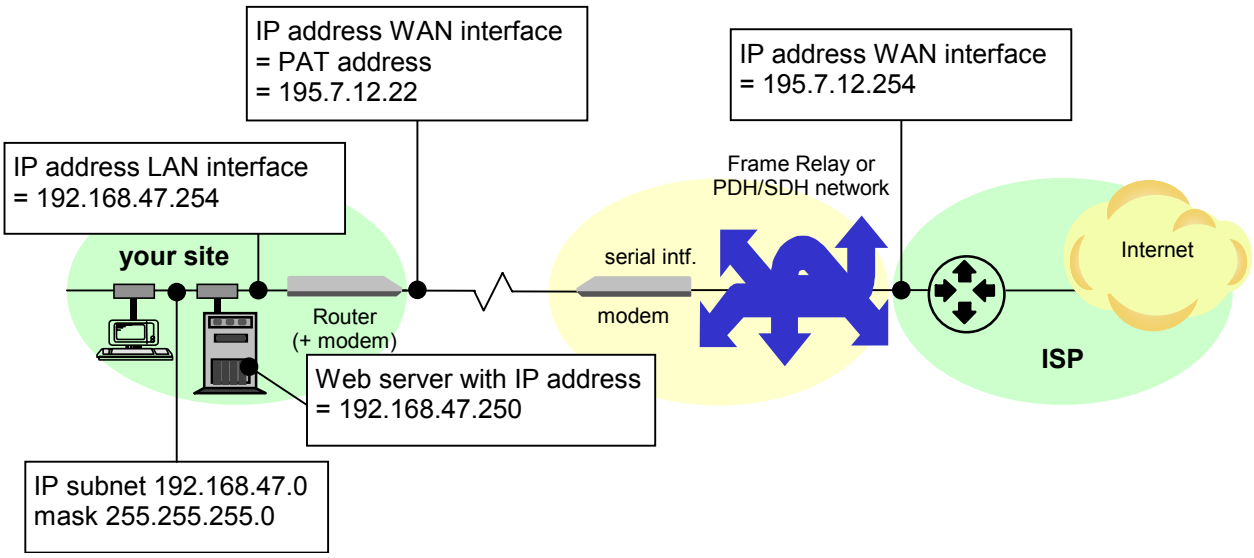
The configuration of the Telindus 1031 Router in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        address = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = atm
      }
      SELECT atm
      {
        LIST
        {
          pvcTable =
          {
            [a] =
            {
              name = pvc1
              ip =
              {
                address = 192.168.100.1
                netmask = 255.255.255.252
                remote = 192.168.100.2
              }
              atm =
              {
                vpi = 100
                vci = 100
              }
            }
          }
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      routingTable =
      {
        [a] =
        {
          network = 192.168.48.0
          gateway = 192.168.100.2
        }
      }
    }
  }
}
action "Activate Configuration"
```

9.4 Connecting a LAN to the Internet using NAT and PAT

This is an example of a local network that only uses private addresses.

A PPP link connects your site to the Internet Service Provider. At your site a Telindus 1031 Router is installed. You only received 2 official IP addresses from the ISP, one for all outgoing traffic using PAT (195.7.12.22) and one for accessing the local web server using NAT (195.7.12.21) with a dedicated private address.



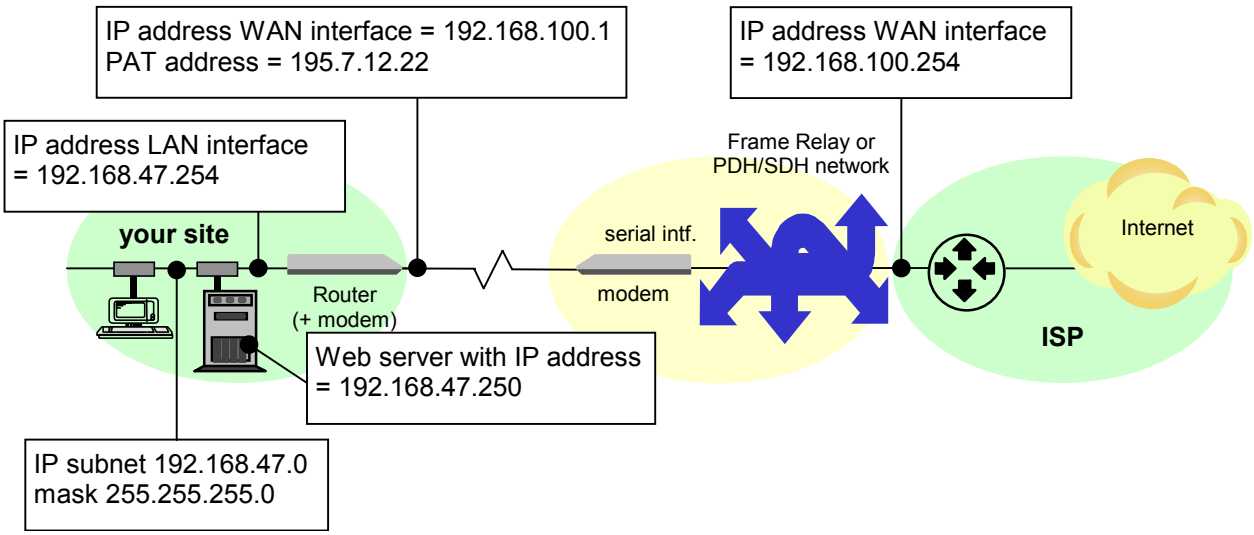
The configuration of the Telindus 1031 Router in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        address = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = ppp
      }
      SELECT ppp
      {
        LIST
        {
          ip =
          {
            address = 195.7.12.22
            nat = default
          }
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      defaultRoute =
      {
        gateway = 195.7.12.254
      }
    }
    SELECT defaultNat
    {
      LIST
      {
        patAddress = 195.7.12.22
        addresses =
        {
          [a] =
          {
            officialAddress = 195.7.12.21
            privateAddress = 192.168.47.250
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

9.5 Using PAT over PPP with a minimum of official IP addresses

This is another example of a local network that only uses private addresses.

A PPP link connects your site to the Internet Service Provider. At your site a Telindus 1031 Router is installed. You only received 1 official IP address from the ISP. To reduce the number of official IP addresses, the ISP also uses private IP addresses on the PPP link. The central router its routing table has a host route to its PAT address per customer.

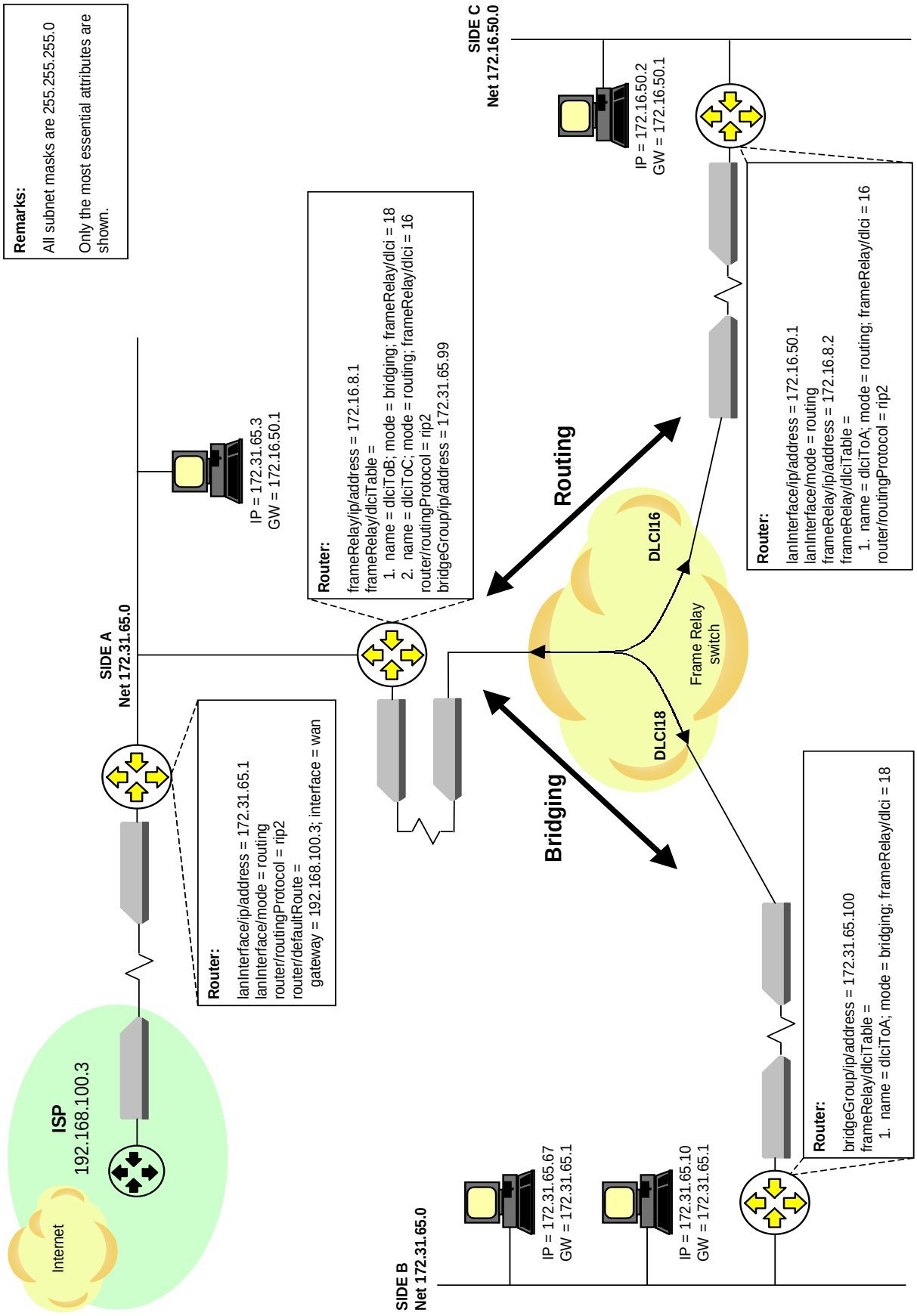


The configuration of the Telindus 1031 Router in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        address = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = ppp
      }
      SELECT ppp
      {
        LIST
        {
          ip =
          {
            address = 192.168.100.1
            nat = default
          }
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      defaultRoute =
      {
        gateway = 192.168.100.254
      }
    }
    SELECT defaultNat
    {
      LIST
      {
        patAddress = 195.7.12.22
        servicesAvailable =
        {
          [a] =
          {
            protocol = tcp
            startPort = 80
            serverAddress = 192.168.47.250
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

9.6 Combining bridging and routing in a network

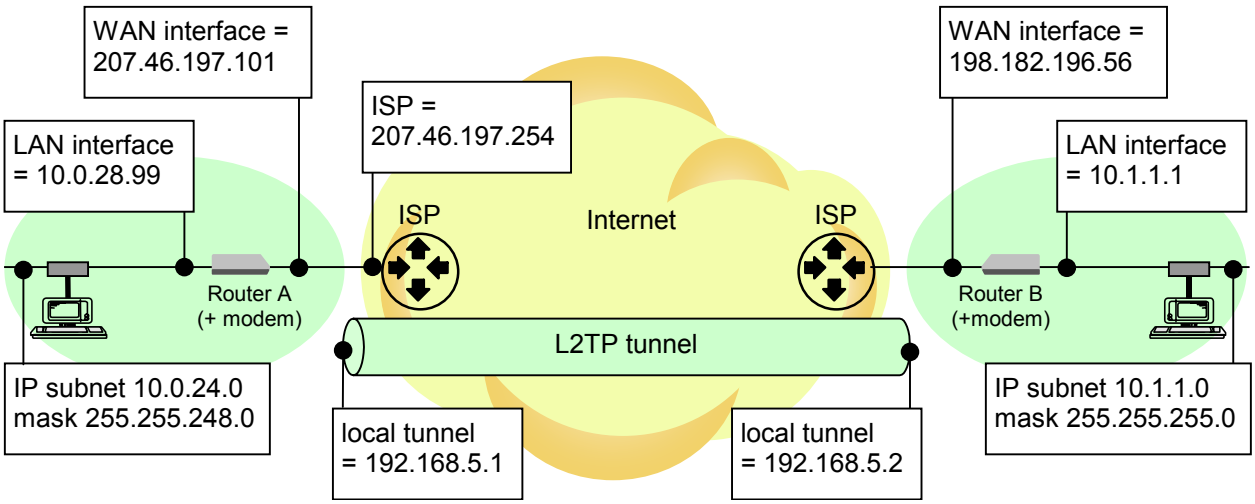
The following example shows a combination of bridging and routing in a network.



9.7 Connecting two networks through a tunnel

This is an example of two networks being connected by two Telindus 1031 Routers through a tunnel over the Internet.

First a route between the WAN interface of Router A and B has to exist. Then the tunnel can be set up. Router A and B learn the routes of each others network through RIP. However, they must not learn the WAN and tunnel IP addresses. Therefore a filter is created.

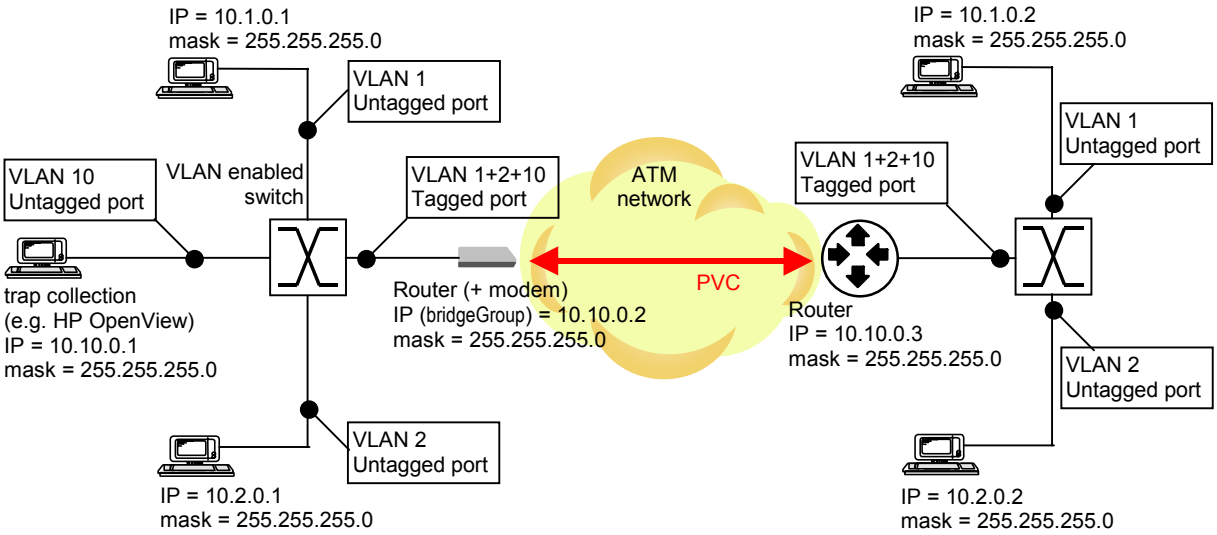


The configuration of Router A in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        address = 10.0.28.99
        netMask = 255.255.248.0
        rip =
        {
          mode = disabled
        }
      }
      mode = routing
    }
  }
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = ppp
      }
      SELECT ppp
      {
        LIST
        {
          ip =
          {
            address = 207.46.197.101
            remote = 207.46.197.254
            rip =
            {
              mode = disabled
            }
          }
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      defaultRoute =
      {
        gateway = 207.46.197.254
      }
      routingProtocol = rip2
    }
    SELECT tunnels
    {
      LIST
      {
        l2tpTunnels =
        {
          [a] =
          {
            name = tunnel1
            ip =
            {
              address = 192.168.5.1
              remote = 192.168.5.2
              rip =
              {
                filter = tunnelFilter
              }
            }
            l2tp =
            {
              localIpAddress = 207.46.197.101
              remoteIpAddress = 198.182.196.56
              type = outgoingLeasedLine
            }
          }
        }
      }
    }
    SELECT routingFilter[tunnelFilter]
    {
      LIST
      {
        filter =
        {
          [a] =
          {
            network = 10.0.0.0
            mask = 255.0.0.0
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

9.8 Connecting VLAN enabled switches over a WAN

This is an example of 2 VLAN enabled switches that connect multiple VLANs over a WAN link. In this example VLAN 10 is used to manage the Telindus 1031 Router and the remote third party router, whereas VLAN 1 and 2 are used for user data. Note that when dotQTagging is enabled, the Telindus 1031 Router does not interpret spanning tree frames. This allows the switches to run the spanning tree protocol themselves as if they were connected directly via Ethernet.



The configuration of the Telindus 1031 Router in CLI format is as follows:

```
action "Load Default Configuration"
SET
{
  SELECT g703[1]
  {
    SELECT channel[g703_1]
    {
      LIST
      {
        encapsulation = atm
      }
      SELECT atm
      {
        LIST
        {
          pvcTable =
          {
            [a] =
            {
              name = pvc1
              mode = bridging
              atm =
              {
                vpi = 100
                vci = 100
              }
            }
          }
        }
      }
    }
  }
  SELECT bridge
  {
    SELECT bridgeGroup
    {
      LIST
      {
        ip =
        {
          address = 10.1.0.2
        }
        vlan =
        {
          dotQTagging = enabled
          vid = 10
        }
      }
    }
  }
}
action "Activate Configuration"
```

Reference manual

10 Configuration attributes

This chapter discusses the configuration attributes of the Telindus 1031 Router. The following gives an overview of this chapter:

- 10.1 - Configuration attribute overview on page 172
- 10.2 - General configuration attributes on page 174
- 10.3 - LAN interface configuration attributes on page 178
- 10.4 - WAN interface configuration attributes on page 181
- 10.5 - Router configuration attributes on page 200
- 10.6 - Bridge configuration attributes on page 231
- 10.7 - SNMP configuration attributes on page 238
- 10.8 - Management configuration attributes on page 240
- 10.9 - Proxy configuration attributes on page 244

10.1 Configuration attribute overview

> telindus1031
- sysName
- sysContact
- sysLocation
- bootFromFlash
- security
- alarmMask
- alarmLevel
- Action: Activate Configuration
- Action: Load Saved Configuration
- Action: Load Default Configuration
- Action: Cold Boot

>> lanInterface
- name
- ip
- arp
- mode
- bridging
- adapter
- alarmMask
- alarmLevel

>> g703[1]
- coding
- framing
- clocking
- crc4Insertion
- longHaul
- jitterAttenuation
- alarmMask
- alarmLevel

>>> channel[g703_1]
- timeSlots
- encapsulation
- priorityPolicy
- maxFifoQLen
- alarmMask
- alarmLevel

>>>> ppp
- ip
- mode
- bridging
- linkMonitoring
- authentication
- authenPeriod

>>>> frameRelay
- ip
- dlciTable
- lmi

>>>> atm
- pvcTable
- atmConfig

>>>> hdlc
- bridging

>> router
- defaultRoute
- routingTable
- routingProtocol
- alternativeRoutes
- ripUpdateInterval
- ripHoldDownTime
- ripv2SecretTable
- sysSecret
- pppSecretTable
- helperProtocols
- sendTtlExceeded
- sendPortUnreachable
- sendAdminUnreachable
- dhcpStatic
- dhcpDynamic
- dhcpCheckAddress
- alarmMask
- alarmLevel

>>> defaultNat
- patAddress
- portTranslations
- servicesAvailable
- addresses
- gateway
- tcpSocketTimeOut
- udpSocketTimeOut
- tcpSockets
- udpSockets
- dmzHost

>>> tunnels
- l2tpTunnels

>>> routingFilter[ ][1]
- filter

>>> trafficPolicy[ ][1]
- method
- trafficShaping
- tos2QueueMapping
- dropLevels

>>> priorityPolicy[ ][1]
- algorithm
- countingPolicy
- queueConfigurations
- lowdelayQuotum

>> bridge

>>> bridgeGroup
- bridgeCache
- bridgeTimeOut
- name
- ip
- arp
- spanningTree
- vlan

>>> accessList[ ][1]
- macAddress

>>> trafficPolicy[ ][1]
- vlanPriorityMap

>> snmp
- trapDestinations
- mib2Traps

>> management
- cms2Address
- accessList
- snmp
- telnet
- tftp
- consoleNoTrafficTimeOut
- ctrlPortProtocol
- alarmFilter

>>> loopback
- ipAddress

>> proxy[1]

Refer to the Telindus 1030 Router Orchid function manual for more information on the configuration attributes of the proxy function (also called Orchid function).

1. Not present by default, has to be added.

10.2 General configuration attributes

telindus1031/sysName

Default:<empty>
Range: 0 … 64 characters

Use this attribute to assign a name to the Telindus 1031 Router. The sysName attribute is an SNMP MIB2 parameter.

telindus1031/sysContact

Default:<empty>
Range: 0 … 64 characters

Use this attribute to add contact information. You could, for instance, enter the name and telephone number of the person to contact in case problem occur.

The sysContact attribute is an SNMP MIB2 parameter.

telindus1031/sysLocation

Default:<empty>
Range: 0 … 64 characters

Use this attribute to specify the physical location of the Telindus 1031 Router. The sysLocation attribute is an SNMP MIB2 parameter.

telindus1031/bootFromFlash

Default:auto
Range: enumerated, see below

Part of the flash memory of the Telindus 1031 Router is organised as a file system. In this file system, you can store two complete application software versions. You can use the bootFromFlash attribute to switch between these softwares.

When you store two application software versions in the file system, they are automatically renamed as CONTROL1 and CONTROL2, respectively. You can check this with the status attribute telindus1031/fileSystem/fileList.

The bootFromFlash attribute has the following values:

Value	When the Telindus 1031 Router boots …
flash1	the application software CONTROL1 is active.
flash2	the application software CONTROL2 is active.
auto	the Telindus 1031 Router automatically chooses the most recent application software. It does this by comparing the application software version numbers.

telindus1031/security

Default:<empty>
Range: table, see below

Use this attribute to create a list of passwords with associated access levels in order to avoid unauthorised access to the Telindus 1031 Router and the network.

The security table contains the following elements:

Element	Description
password	Use this element to set the password. You can then associate this password with a certain access level. Default:<empty> Range: 0 … 10 characters
accessRights	Use this element to set the access level associated with the password. It is a bit string of which each bit corresponds to an access level. The different access levels are listed below. Default:1111 Range: bit string, see below

The following table shows, for each access level, what you can or can not do:

Access level	Read attributes	Change attributes	Read security attributes[1]	Change security attributes	Execute actions[2]	Access file system
readAccess	yes	no	no	no	no	no
writeAccess	yes	yes	no	no	yes	no
securityAccess	no	no	yes	yes	no	no
fileSystem-Access	no	no	no	no	no	yes

1. The Telindus 1031 Router has the following security attributes:
   telindus1031/sysName
   telindus1031/security
   telindus1031/router/sysSecret, pppSecretTable and ripv2SecretTable
   telindus1031/router/priorityPolicy and trafficPolicy
   telindus1031/wanInterface/ppp/authentication and authenPeriod
   telindus1031/management/accessList, snmp, telnet and tftp
2. Actions are e.g. Cold Boot, clearArpCache, clearBridgeCache, etc…

Important remarks

- If you create no passwords, everybody has complete access.
- If you define at least one password, it is impossible to access the Telindus 1031 Router with one of the management systems without entering the correct password.
- If you create a list of passwords, create at least one with write and security access. If not, you will be unable to make configuration and password changes after activation of the new configuration.

telindus1031/alarmMask

telindus1031/alarmLevel

Refer to …

- 13.2 - Introducing the alarm attributes on page 329 for more information on the configuration attributes alarmMask and alarmLevel and on the alarms in general.
- 13.3 - General alarms on page 332 for more information on the alarms of the telindus1031 object.

telindus1031/Activate Configuration

If you execute this action, the editable non-active configuration becomes the active configuration. This action corresponds with the TMA button *Send all attributes to device*: .

When use this action?

Use this action after you made all the necessary configuration settings and you want to activate these settings.

telindus1031/Load Default Configuration

If you execute this action, the non-active configuration is overwritten by the default configuration.

After executing this action, click on the TMA button *Retrieve all attributes from device* to see the new non-active configuration.

When use this action?

If you install the Telindus 1031 Router for the first time, all configuration attributes have their default values. If the Telindus 1031 Router has already been configured but you want to start from scratch, then use this action to revert to the default configuration.

telindus1031/Load Saved Configuration

If you execute this action, the non-active configuration is overwritten by the active configuration currently used by the Telindus 1031 Router.

After executing this action, click on the TMA button *Retrieve all attributes from device* to see the new non-active configuration.

When use this action?

If you are in the progress of modifying the non-active configuration but made some mistakes, then use this action to revert to the active configuration.

telindus1031/Cold Boot

If you execute this action, the Telindus 1031 Router reboots. As a result, the Telindus 1031 Router …

- performs a self-test.
- checks the software.
- reads the saved configuration and restarts program execution.

When use this action?

Use this action, for instance, to activate new application software.

10.3 LAN interface configuration attributes

telindus1031/lanInterface/name

Default:lan
Range: 1 … 24 characters

Use this attribute to assign an administrative name to the LAN interface.

telindus1031/lanInterface/ip

Default:-
Range: structure, see below

Use this attribute to configure the IP related parameters of the LAN interface.

Important remark

If you set the configuration attribute telindus1031/lanInterface/mode to bridging, then the settings of the configuration attribute telindus1031/lanInterface/ip are ignored. As a result, if you want to manage the Telindus 1031 Router via IP, you have to configure an IP address in the bridgeGroup object instead: telindus1031/bridge/bridgeGroup/ip.

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

telindus1031/lanInterface/arp

Default:-
Range: structure, see below

Use this attribute to configure the Address Resolution Protocol (ARP) cache.

The arp structure contains the following elements:

Value	Description	
timeOut	Use this element to set the ageing time of the ARP cache entries. Refer to The ARP cache time-out.	Default:00000d 02h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
proxyArp	Use this element to enable or disable the ARP cache mechanism.	Default:enabled Range: enabled / disabled

What is the ARP cache?

The LAN interface has been allocated a fixed Ethernet address, also called MAC (Medium Access Control) address. This MAC address is not user configurable. The IP address of the LAN interface, on the other hand, is user configurable. This means that the user associates an IP address with the predefined MAC address. The MAC address - IP address pairs are kept in a table, called the ARP cache. Refer to telindus1031/lanInterface/arpCache on page 253 for an example of such a table.

How does the ARP cache work?

Before the Telindus 1031 Router sends an IP packet on the LAN interface, it has to know the MAC address of the destination device. If the address is not present in the ARP cache table yet, the Telindus 1031 Router sends an ARP request on the Ethernet to learn the MAC address and associated IP address of the destination device. This address pair is then written in the ARP cache. Once the address pair is present, the Telindus 1031 Router can reference to this pair if it has to send an IP packet to the same device later on.

The ARP cache time-out

Summarised, all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface are kept in the ARP cache. However, if devices on the network are reconfigured then this MAC address - IP address relation may change. Therefore, the ARP cache entries are automatically removed from the cache after a fixed time-out. This time-out period can be set with the timeOut element.

telindus1031/lanInterface/mode

Default:bridging
Range: enumerated, see below

Use this attribute to determine whether the packets are treated by the routing process, the bridging process or both.

The mode attribute has the following values:

Value	Description
bridging	All packets are bridged. The settings of the IP configuration attributes of the LAN are ignored. If you want to manage the Telindus 1031 Router via IP, you have to configure an IP address in the bridgeGroup object. Refer to telindus1031/bridge/bridgeGroup/ip on page 233.
routing	The IP packets are routed. All other protocols are discarded.
routingAndBridging	IP packets are routed. Non-IP packets are bridged. The settings of the IP configuration attributes are taken into account.

telindus1031/lanInterface/bridging

Default:-
Range: structure, see below

Use this attribute to configure the bridging related parameters of the LAN interface.

Refer to …

- 8 - Configuring the bridge on page 139 for more information on bridging.
- 8.9.6 - Explaining the bridging structure on page 152 for a detailed description of the bridging structure.

telindus1031/lanInterface/adapter

Default:autoDetect
Range: enumerated, see below

Use this attribute to set the Ethernet mode of the LAN interface.

The adapter attribute has the following values: autoDetect, 10Mb/halfDuplex, 10Mb/fullDuplex, 100Mb/halfDuplex.

telindus1031/lanInterface/alarmMask

telindus1031/lanInterface/alarmLevel

Refer to …

- 13.2 - Introducing the alarm attributes on page 329 for more information on the configuration attributes alarmMask and alarmLevel and on the alarms in general.
- 13.4 - LAN interface alarms on page 334 for more information on the alarms of the lanInterface object.

10.4 WAN interface configuration attributes

This section discusses the configuration attributes of the WAN interface. First it describes the configuration attributes of the physical interface. Then it explains the configuration attributes of the encapsulation protocols that can be used on the interface.

The following gives an overview of this section:

- 10.4.1 - G703 interface configuration attributes on page 182
- 10.4.2 - G703 channel configuration attributes on page 184
- 10.4.3 - PPP configuration attributes on page 185
- 10.4.4 - Frame Relay configuration attributes on page 188
- 10.4.5 - ATM configuration attributes on page 193
- 10.4.6 - HDLC configuration attributes on page 199

10.4.1 G703 interface configuration attributes

telindus1031/g703[ ]/coding

Default:hdb3
Range: enumerated, see below

Use this attribute to set the G703 interface encoding mode.

The coding attribute has the following values:

Value	Description
ami	Alternate Mark Inversion is selected. This is a bipolar code with no zero substitution.
hdb3	High Density Bipolar 3 is selected. This is a modified bipolar code. In case of HDB3 encoding, if more than three consecutive zeroes occur in the data they are replaced by a substitution word. This ensures a high pulse density. Therefore, data links using the HDB3 code can carry data patterns with a low 1 density. Most of the G703 applications use HDB3 encoding.

telindus1031/g703[ ]/framing

Default:unframed
Range: enumerated, see below

Use this attribute to select between unframed or framed mode.

The framing attribute has the following values:

Value	Description
unframed	In unframed (transparent) mode, a 2 Mbps data stream is sent transparently over the line. In this mode, the attributes telindus1031/g703[ ]/crc4Insertion and telindus1031/g703[ ]/channel[ ]/timeSlots are of no use and may be ignored.
framed	In framed (G.704 framing) mode, up to 32 time slots each containing a 64 kbps data stream can be sent over the line. Each 64 kbps time slot can be enabled or disabled individually. Refer to telindus1031/g703[ ]/channel[ ]/timeSlots on page 184.

telindus1031/g703[ ]/clocking

Default:slaveReceive
Range: enumerated, see below

Use this attribute to select a clocking mode.

The clocking attribute has the following values:

Value	Description
slaveReceive	The transmit data is clocked out with the clock retrieved from the receive data.
internal	The transmit data is clocked out at an internal clock rate.

telindus1031/g703[ ]/crc4Insertion

Default:auto
Range: enumerated, see below

Use this attribute to determine whether the CRC-4 (Cyclic Redundancy Check) is recalculated before sending it to the interface. The CRC is used to check the data integrity on the G.703 connection.

The crc4Insertion attribute has the following values:

Value	Description
auto	In auto mode, CRC-4 insertion is … • disabled if the speed matches 2 Mbps. • enabled if the speed differs from 2 Mbps.
disabled	CRC-4 insertion is disabled.
enabled	CRC-4 insertion is enabled.

telindus1031/g703[ ]/longHaul

Default:disabled
Range: enabled / disabled

Use this attribute to enable or disable the long haul driver.

When you enable the driver, you can cover long distances. The distances are in the order of:

- 2.5 km when using a cable with a diameter of 0.6 mm.
- 1.25 km when using a cable with a diameter of 0.4 mm.

telindus1031/g703[ ]/jitterAttenuation

Default:32Bits
Range: enumerated, see below

Use this attribute to set the buffer depth of the jitter attenuator. The jitter attenuator of the Telindus 1031 Router attenuates the clock and data jitter.

The values of the jitterAttenuation attribute are 32Bits and 128Bits. You may wish to limit the buffer size to 32 bits in applications where throughput delay is critical.

telindus1031/g703[ ]/alarmMask

telindus1031/g703[ ]/alarmLevel

Refer to …

- 13.2 - Introducing the alarm attributes on page 329 for more information on the configuration attributes alarmMask and alarmLevel and on the alarms in general.
- 13.5 - G703 interface alarms on page 335 for more information on the alarms of the g703[ ] object.

10.4.2 G703 channel configuration attributes

telindus1031/g703[ ]/channel[ ]/timeSlots

Default:all time slots disabled
Range: bit string, see below

Use this attribute to enable or disable the individual 64 kbps time slots in the framed data stream.

telindus1031/g703[ ]/channel[ ]/encapsulation

Default:atm
Range: enumerated, see below

Use this attribute to select the encapsulation protocol on the WAN interface.

The encapsulation attribute has the following values: frameRelay, ppp, atm and hdlc.

Important remark

You can only use ATM encapsulation on the G703 interface when you selected framed mode, not when you selected unframed mode (refer to telindus1031/g703[ ]/framing on page 182).

telindus1031/g703[ ]/channel[ ]/priorityPolicy

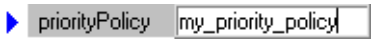
Default:<empty>
Range: 0 … 24 characters

Use this attribute to apply a priority policy on the interface.

Do this by entering the index name of the priority policy you want to use. You can create the priority policy itself by adding a priorityPolicy object under the router object and by configuring the attributes in this object.

Example

If you created a priorityPolicy object with index name my_priority_policy (i.e. priorityPolicy[my_priority_policy]) and you want to apply this priority policy here, then enter the index name as value for the priorityPolicy attribute.



Refer to …

- 7.6.5 - Configuring a priority policy on page 135 for more information on priority policies.
- 4.4 - Adding an object to the containment tree on page 45 for more information on adding objects.

telindus1031/g703[ ]/channel[ ]/maxFifoQLen

Default:<empty>
Range: 0 … 24 characters

Use this attribute to set the maximum length (number of packets) of the First In First Out queue.

Refer to telindus1031/router/priorityPolicy[ ]/algorithm on page 228 for more information on this queue.

telindus1031/g703[ ]/channel[ ]/alarmMask

telindus1031/g703[ ]/channel[ ]/alarmLevel

Refer to …

- 13.2 - Introducing the alarm attributes on page 329 for more information on the configuration attributes alarmMask and alarmLevel and on the alarms in general.
- 13.6 - G703 channel alarms on page 336 for more information on the alarms of the g703[ ]/channel[ ] object.

10.4.3 PPP configuration attributes

telindus1031/g703[ ]/channel[ ]/ppp/ip

Default:<empty>
Range: structure, see below

Use this attribute to configure the IP related parameters of the PPP link.

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

telindus1031/g703[ ]/channel[ ]/ppp/mode

Default:bridging
Range: enumerated, see below

Use this attribute to determine whether the packets are treated by the routing process, the bridging process or both.

The mode attribute has the following values:

Value	Description
bridging	All packets received on the PPP link are bridged. BCP is set up.
routing	All packets received on the PPP link are routed. IPCP is set up.
routingAndBridging	The SNAP header is checked to determine whether the packets have to be bridged or routed. IPCP and BCP is set up.

telindus1031/g703[ ]/channel[ ]/ppp/bridging

Default:-
Range: structure, see below

Use this attribute to configure the bridging related parameters of the PPP link.

Refer to …

- 8 - Configuring the bridge on page 139 for more information on bridging.
- 8.9.6 - Explaining the bridging structure on page 152 for a detailed description of the bridging structure.

telindus1031/g703[ ]/channel[ ]/ppp/linkMonitoring

Default:-
Range: structure, see below

Use this attribute to enable or disable link monitoring and to fine-tune it.

Refer to 6.2.3 - Configuring link monitoring on page 75 for more information on link monitoring.

The linkMonitoring structure contains the following elements:

Element	Description
operation	Use this element to enable or disable link monitoring. Default:disabled Range: enabled / disabled
interval	Use this element to set the time interval between two consecutive echo requests. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
replyTimeOut	Use this element to set the time the Telindus 1031 Router waits for a reply on the echo request. If no reply has been received within this time-out, then the Telindus 1031 Router considers this as a failed echo request. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 00h 04m 15s
failsPermitted	Use this element to set the number of failed echo requests after which the Telindus 1031 Router declares the WAN link down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If on 10 consecutive echo requests no reply is given, then the Telindus 1031 Router declares the WAN link down and the PPP handshake is started again.

telindus1031/g703[ ]/channel[ ]/ppp/authentication

Default:disabled
Range: enumerated, see below

Use this attribute to enable or disable CHAP authentication on the PPP link.

Refer to 6.2.4 - Configuring PPP authentication on page 76 for more information on authentication.

The authentication attribute has the following values:

Value	Description
disabled	Authentication is disabled.
chap	This side of the link requests a CHAP authentication from the remote router.

telindus1031/g703[ ]/channel[ ]/ppp/authenPeriod

Default:00000d 00h 10m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to set the PPP authentication interval.

Refer to 6.2.4 - Configuring PPP authentication on page 76 for more information on authentication.

Normally on an authenticated PPP link, authentication is not only performed at link set-up but also at regular intervals during the data transfer. You can set this interval using the authenPeriod attribute. If you set the authenPeriod attribute to 00000d 00h 00m 00s, then authentication is only performed at link set-up and not during the data transfer.

10.4.4 Frame Relay configuration attributes

telindus1031/g703[ ]/channel[ ]/frameRelay/ip

Default:<empty>
Range: structure, see below

Use this attribute to globally configure the IP parameters of the DLCIs. More specifically, use this attribute to configure the IP related parameters of all the DLCIs for which …

- in the dlciTable no IP address is defined for that specific DLCI,
- and the mode element is set to routing or routingAndBridgning.

If you want to configure the IP related parameters for one specific DLCI, then configure for that DLCI the ip structure in the dlciTable.

Refer to …

- 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.
- 6.3.2 - Configuring IP addresses on the Frame Relay WAN on page 80 for more specific information on configuring IP addresses in Frame Relay.

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable

Default:<empty>
Range: table, see below

Use this attribute to configure the Frame Relay Data Link Connection Identifiers (DLCIs).

Refer to 6.3.3 - Configuring the DLCIs on page 83 for more information on DLCIs.

The dlciTable contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the DLCI. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate (down) the DLCI. Default:up Range: up / down
mode	Use this element to determine whether, for the corresponding DLCI, the packets are treated by the routing process, the bridging process or both. Default:routing Range: enumerated, see below The mode element has the following values: **Value** / **Description** bridging: All packets received on the DLCI are bridged. routing: All packets received on the DLCI are routed. routingAndBridging: The SNAP header is checked to determine whether the packets have to be bridged or routed.
ip	Use this element to configure the IP related parameters of the corresponding DLCI. Default:- Range: structure, see below Refer to … • 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure. • 6.3.2 - Configuring IP addresses on the Frame Relay WAN on page 80 for more specific information on configuring IP addresses in Frame Relay.
bridging	Use this element to configure the bridging related parameters of the DLCI. Default:- Range: structure, see below Refer to … • 8 - Configuring the bridge on page 139 for more information on bridging. • 8.9.6 - Explaining the bridging structure on page 152 for a detailed description of the bridging structure.
frameRelay	Use this element to configure the specific DLCI parameters. Default:- Range: structure, see below Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay on page 190, for a detailed description of the frameRelay structure.

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay

Default:-
Range: structure, see below

Use the frameRelay structure in the dlciTable to configure the Frame Relay related parameters of the corresponding DLCI.

Refer to …

- 6.3.3 - Configuring the DLCIs on page 83 for more information on DLCIs.
- 6.3.5 - Configuring CIR and EIR on page 85 for more information on CIR and EIR.

The frameRelay structure contains the following elements:

Element	Description
dlci	Use this element to set the DLCI number to reach a remote network. Default:16 Range: 16 … 1022 The DLCI number may have any value between 16 and 1022. However, if you set the configuration attribute lmi to q933-Annex-A, you should only use DLCIs up to 1007.
cir	Use this element to set the Committed Information Rate for the DLCI. Default:0 Range: 0 … 2048000 The CIR is expressed in bps. Any value between 0 and 2048000 (bps) can be configured. If the cir value is set to 0 (default), it means the complete bandwidth may be used (no flow control).
eir	Use this element to set the Excess Information Rate for the DLCI. Default:0 Range: 0 … 2048000 The EIR is expressed in bps. Any value between 0 and 2048000 (bps) can be configured. If the eir value is set to 0 (default), it means no excess burst is allowed. The bursts of data that are allowed are the CIR value + EIR value. I.e. If you want a CIR of 1 Mbps and you want to allow bursts up to 1.5 Mbps, then set the CIR to 1024000 bps and the EIR to 512000 bps.

telindus1031/g703[ ]/channel[ ]/frameRelay/lmi

Default:-
Range: structure, see below

Use this attribute to select the Local Management Interface (LMI) protocol and to fine-tune the LMI operation.

Refer to 6.3.4 - Configuring LMI on page 84 for more information on LMI.

The lmi structure contains the following elements:

Element	Description
mode	Use this element to set the Frame Relay mode. Default:auto Range: enumerated, see below The mode element has the following values: **Value** / **Description** noLmi — No LMI is used. user — The Telindus 1031 Router is defined as Frame Relay user. I.e. Frame Relay access device or DTE. network — The Telindus 1031 Router is defined as Frame Relay network. I.e. Frame Relay node or DCE. auto — When you have two Telindus 1031 Routers in your network and they are both set to auto, they mutually decide who will be user or network.
type	Use this element to set the LMI variant. There are several standards for the LMI protocol with small variations between them. Therefore you should configure the Telindus 1031 Router according to the standard that is used by your service provider. Default:q933-Annex-A Range: enumerated, see below The type element has the following values: **Value** / **Description** lmiRev1 — Set this value only for compatibility with older equipment. ansiT1-617-d — Set this value for ANSI LMI compliance. q933-Annex-A — Set this value for ITU-T LMI compliance. frf1-2 — Set this value for FRF 1 & 2 compliance.
pollingInterval	Use this element to set the time between successive Status Enquiry messages. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 05s - 00000d 00h 00m 30s
errorThreshold	Use this element to set the maximum number of unanswered Status Enquiry messages that the Telindus 1031 Router will accept before declaring the DLCI down. Also see the monitoredEvents element. Default:3 Range: 1 … 10

Element	Description
monitoredEvents	Use this element to set the number of status polling intervals over which the error threshold is counted. Default:4 Range: 1 … 10 In other words, if the station receives an errorThreshold number of unanswered Status Enquiry messages within a monitoredEvents number of pollingInterval intervals, then the interface is declared down. **Example** If the station receives 3 unanswered Status Enquiry messages within 4 x 10s = 40s, then the interface is declared down.
expectedPollInterval	Use this element to set the maximum time between two consecutive incoming Status Enquiry messages. Select the value 0 in order to disable verification. Default:00000d 00h 00m 15s Range: 00000d 00h 00m 00s - 00000d 00h 00m 30s This element is only relevant when using Frame Relay over a point-to-point link (no Frame Relay network). In Frame Relay language, a router is normally considered as a DTE. However, if two routers are connected to each other in Frame Relay but without a real Frame Relay network in between, then the routers also take the role of a DCE (refer to the mode element). The Status Enquiry messages are sent in both directions.
fullEnquiryInterval	Use this element to set the number of Status Enquiry intervals that have to elapse before sending a Full Status Enquiry message. Default:6 Range: 1 … 255

10.4.5 ATM configuration attributes

Important remark

You can only use ATM encapsulation on the G703 interface when you selected framed mode, not when you selected unframed mode (refer to telindus1031/g703[ ]/framing on page 182).

telindus1031/g703[ ]/channel[ ]/atm/pvcTable

Default:<empty>
Range: table, see below

Use this attribute to configure the ATM Permanent Virtual Circuits (PVCs).

Refer to 6.4.3 - Configuring the PVCs on page 90 for more information on PVCs.

The pvcTable contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the PVC. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate (down) the PVC. Default:up Range: up / down
mode	Use this element to determine whether, for the corresponding PVC, the packets are treated by the routing process, the bridging process or both. Default:routing Range: enumerated, see below The mode element has the following values:
priorityPolicy	Use this element to set a priority policy per PVC. Refer to telindus1031/g703[ ]/channel[ ]/priorityPolicy on page 184 for more information. Default:<empty> Range: 0 … 24 characters
ip	Use this element to configure the IP related parameters of the PVC. Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure. Default:- Range: structure, see below

Value	Description
bridging	All packets received on the PVC are bridged.
routing	All packets received on the PVC are routed.
routingAndBridging	The SNAP header is checked to determine whether the packets have to be bridged or routed.

Element	Description
bridging	Use this element to configure the bridging related parameters of the PVC. Default:- Range: structure, see below Refer to … • 8 - Configuring the bridge on page 139 for more information on bridging. • 8.9.6 - Explaining the bridging structure on page 152 for a detailed description of the bridging structure.
atm	Use this element to configure the specific PVC parameters. Default:- Range: structure, see below Refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm on page 195 for a detailed description of the atm structure.
ppp	Use this element to configure the PPP related parameters of the PVC in case you choose to map PPP onto AAL5 (refer to the elements higherLayerProtocol and multiProtocolMech on page 195). Default:- Range: structure, see below For a detailed description of the elements in the ppp structure, refer to … • telindus1031/g703[ ]/channel[ ]/ppp/linkMonitoring on page 186, • telindus1031/g703[ ]/channel[ ]/ppp/authentication on page 187, • telindus1031/g703[ ]/channel[ ]/ppp/authenPeriod on page 187.

telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm

Default:-
Range: structure, see below

Use the atm structure in the pvcTable to configure the ATM related parameters of the corresponding PVC.

Refer to 6.4.3 - Configuring the PVCs on page 90 for more information on PVCs.

The atm structure contains the following elements:

Element	Description
vpi	Use this element to set the Virtual Path Identifier (VPI). Default:0 Range: 0 … 255
vci	Use this element to set the Virtual Channel Identifier (VCI). Default:32 Range: 32 … 65535 The VPI in conjunction with the VCI identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
higherLayerProtocol	Use this element to define which protocol has to be mapped onto the ATM Adaptation Layer 5 (AAL5). Default:rfc2684 Range: enumerated, see below The higherLayerProtocol element has the following values:

Value	Description
rfc2684	Select this value in case you want to encapsulate routed or bridged data in AAL5 packets according to RFC2684.
ppp	Select this value in case you want to encapsulate routed or bridged data in PPP over ATM (PPPoA) according to RFC2364.
pppOverEthernet	Select this value in case you want to encapsulate routed or bridged data in PPP over Ethernet (PPPoE) according to RFC2516. This data is then further encapsulated in AAL5 packets according to RFC2684. In the PPPoE context, the Telindus 1031 Router can only act as a client.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>multiProtocolMech</td><td>Use this element to define how the protocol has to be mapped onto ATM Adaptation Layer 5 (AAL5).
Default:llcEncapsulation
Range: enumerated, see below

The multiProtocolMech element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>llcEncapsulation</td><td>Logical Link Control (LLC) encapsulation multiplexes multiple protocols over a single virtual circuit. The protocol of a carried protocol data unit (PDU) is identified by prefixing the PDU with an LLC header.</td></tr>
<tr><td>vcMultiplexing</td><td>Virtual Circuit (VC) based multiplexing uses one Virtual Channel (VCI/VPI pair) for each protocol. This uses more VCs than LLC encapsulation, but reduces overhead, because a header is not necessary.</td></tr>
</table>

The following table gives an overview of which multi-protocol mechanism can be used for which higher layer protocol encapsulation. It also shows whether this can be combined with NAT/PAT.

<table>
<tr><th>Device as router or bridge?</th><th>higherLayerProtocol</th><th>multiProtocolMech</th><th>NAT/PAT support</th></tr>
<tr><td rowspan="3">router</td><td>rfc2684</td><td>llcEncapsulation</td><td>yes</td></tr>
<tr><td>ppp</td><td>llcEncapsulation + vcMultiplexing</td><td>yes</td></tr>
<tr><td>pppOverEthernet</td><td>llcEncapsulation</td><td>yes</td></tr>
<tr><td rowspan="3">bridge</td><td>rfc2684</td><td>llcEncapsulation</td><td>no</td></tr>
<tr><td>ppp</td><td>llcEncapsulation + vcMultiplexing</td><td>no</td></tr>
<tr><td>pppOverEthernet</td><td>llcEncapsulation</td><td>no</td></tr>
</table>
</td></tr>
<tr><td>peakCellRate</td><td>Use this element to set the maximum bandwidth of the PVC.
Default:auto
Range: enumerated, see below

The peakCellRate element has the following values: auto and 64kbps up to 2304kbps in steps of 64kbps. In auto mode, the PVC will try to get the maximum bandwidth, i.e. the speed of the physical connection towards the ATM network.Refer to 6.4.4 - Configuring the PCR on page 91 for more information on the peak cell rate.</td></tr>
<tr><td>inArpTimeOut</td><td>Use this element to set the time between the transmission of two consecutive Reverse ARP frames.
Default:00000d 00h 00m 30s
Range: 00000d 00h 00m 01s - 00000d 01h 00m 00s</td></tr>
<tr><td>oamF5Loopback</td><td>Use this element to configure the transmission of OAM F5 loop-back cells.
Default:-
Range: structure, see below

Refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm/oamF5Loopback on page 197 for a detailed description of the oamF5Loopback structure.</td></tr>
</table>

telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm/oamF5Loopback

Default:-
Range: structure, see below

Use the oamF5Loopback structure in the atm structure (in the pvcTable) to configure the transmission of OAM F5 loop-back cells.

The oamF5Loopback structure contains the following elements:

Element	Description
operation	Use this element to enable or disable OAM F5 loop-back operation. Default:disabled Range: enabled / disabled The operation element has the following values: **Value** / **Description** disabled: OAM F5 loop-back operation is disabled, i.e. the OAM F5 loop-back are not sent. This means that the ifOperStatus of the PVC becomes up when the ATM is synchronised globally. However, this does not guarantee that the PVC is configured (correctly) on the remote side. enabled: OAM F5 loop-back operation is enabled, i.e. the Telindus 1031 Router sends OAM F5 loop-back cells at regular intervals. If consecutive cells are not returned by the remote side, then the ifOperStatus of the PVC becomes down.
interval	Use this element to set the time interval between the sending of two consecutive OAM F5 loop-back cells. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
failsPermitted	Use this element to set the number of non-returned OAM F5 loop-back cells after which the Telindus 1031 Router declares the PVC down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If 10 consecutive OAM F5 loop-back cells are not returned by the remote side, then the Telindus 1031 Router declares the PVC down.

What are OAM F5 loop-back cells?

The ATM protocol features OAM F5 loop-back cells. These are used to verify whether a PVC is truly up or down. Refer to the operation element in the attribute telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm/oamF5Loopback.

telindus1031/g703[ ]/channel[ ]/atm/atmConfig

Default:-
Range: structure, see below

Use this attribute to configure the general ATM parameters.

The atmConfig structure contains the following elements:

Element	Description
idleCellFormat	Use this element to set the format of the ATM idle cells. These cells are transmitted when no data is transmitted over the line. I.e. the line is idle. Default:itu Range: enumerated, see below The idleCellFormat element has the following values: **Value** / **Description** itu — Sets the cells according to the ITU-T format. In this case they are effectively called “idle cells”. atmForum — Sets the cells according to the ATM forum format. In this case they are actually called “unassigned cells”. Some devices use the ITU-T format, others the ATM forum format. Should the performance attribute telindus1031/g703[ ]/channel[ ]/atm/unknownCells increase rapidly, then try selecting a different format. However, the default value suffices in most cases.
scrambling	Use this element to enable or disable scrambling. Default:enabled Range: enabled / disabled Scrambling is designed to randomise the pattern of 1s and 0s carried in ATM cells or the physical layer frame. Randomising the digital bits can prevent continuous, non-variable bit patterns, in other words long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.
coset	Use this element to enable or disable coset. Default:enabled Range: enabled / disabled Coset is an ATM parameter which indicates when to calculate the header error correction bit if it is to be “OR”ed with another value or not (known as the COSET Polynomial).

10.4.6 HDLC configuration attributes

telindus1031/g703[ ]/channel[ ]/hdlc/bridging

Default:-
Range: structure, see below

Use this attribute to configure the bridging related parameters of the HDLC link.

Refer to …

- 8 - Configuring the bridge on page 139 for more information on bridging.
- 8.9.6 - Explaining the bridging structure on page 152 for a detailed description of the bridging structure.

10.5 Router configuration attributes

This section discusses the configuration attributes concerned with routing. First it describes the general routing configuration attributes. Then it explains the configuration attributes of the extra features as there are default NAT, L2TP tunnelling, filtering, traffic and priority policy, etc…

The following gives an overview of this section:

- 10.5.1 - General router configuration attributes on page 201
- 10.5.2 - Default NAT configuration attributes on page 215
- 10.5.3 - L2TP tunnel configuration attributes on page 218
- 10.5.4 - Routing filter configuration attributes on page 222
- 10.5.5 - Traffic policy configuration attributes on page 223
- 10.5.6 - Priority policy configuration attributes on page 228

10.5.1 General router configuration attributes

telindus1031/router/defaultRoute

Default:-
Range: structure, see below

Use this attribute to set the default route, also called gateway address.

Refer to 7.2 - Configuring static routes on page 100 for more information on static routes.

The defaultRoute structure contains the following elements:

Element	Description
gateway	Use this element to specify the IP address of the next router that will route all packets for which no specific (static or dynamic) route exists in the routing table. Default:0.0.0.0 Range: up to 255.255.255.255 Whether you can omit the gateway element or not, is linked to the following conditions: **If the interface element specifies …** / **then …** the LAN interface, / you can not omit the gateway element. the WAN interface, / you can omit the gateway element only when using PPP encapsulation. a DLCI, PVC or tunnel, / you can omit the gateway element.
interface	Use this element to specify the interface through which the gateway can be reached. Default:<empty> Range: 0 … 24 characters Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus1031/lanInterface/name). Note that this interface can also be a DLCI, PVC, tunnel, etc. If you do not specify a value for the interface element, then it is deduced by checking all interfaces (including DLCIs, PVCs and tunnels) and finding an interface for which the gateway lies in the subnet defined by the IP address and net mask of that interface. Typing the string “discard”, discards all packets for the corresponding destination.
preference	Use this element to set the level of importance of the default route with respect to routes learnt via RIP. Default:10 Range: 1 … 200 RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.
metric	Use this element to set with how much the metric parameter of a route has to be incremented. Default:1 Range: 1 … 15 If two routes exist with the same preference, then the route with the lowest metric value is chosen. This element is only important when combining static routes and RIP routes. Refer to 7.3.3 - Explaining the rip structure on page 110 for more information on the metric parameter.

telindus1031/router/routingTable

Default:<empty>
Range: table, see below

Use this attribute to configure the static IP routes.

Refer to 7.2 - Configuring static routes on page 100 for more information on static routes.

The routingTable table contains the following elements:

Element	Description
network	Use this element to specify the IP address of the destination network. Default:0.0.0.0 Range: up to 255.255.255.255
mask	Use this element to specify the network mask of the destination network. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	Use this element to specify the IP address of the next router on the path to the destination network. Default:0.0.0.0 Range: up to 255.255.255.255 Whether you can omit the gateway element or not, is linked to the following conditions: **If the interface element specifies …** / **then …** the LAN interface, / you can not omit the gateway element. the WAN interface, / you can omit the gateway element only when using PPP encapsulation. a DLCI, PVC or tunnel, / you can omit the gateway element.
interface	Use this element to specify the interface through which the destination network can be reached. Default:<empty> Range: 0 … 24 characters Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus1031/lanInterface/name on page 178). Note that the “interface” can also be a DLCI, PVC, tunnel, etc. If you do not specify a value for the interface element, then it is deduced by checking all interfaces (including DLCIs, PVCs and tunnels) and finding an interface for which the gateway lies in the subnet defined by the IP address and net mask of that interface. Typing the string “discard”, discards all packets for the corresponding destination.
preference	Use this element to set the level of importance of the route with respect to routes learnt via RIP. Default:10 Range: 1 … 200 RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.

Element	Description
metric	Use this element to set with how much the metric parameter of a route has to be incremented. Default:1 Range: 1 … 15 If two routes exist with the same preference, then the route with the lowest metric value is chosen. This element is only important when combining static routes and RIP routes. Refer to 7.3.3 - Explaining the rip structure on page 110 for more information on the metric parameter.

telindus1031/router/routingProtocol

Default:none
Range: enumerated, see below

Use this attribute to activate or deactivate the Routing Information Protocol (RIP).

Refer to 7.3 - Configuring the Routing Information Protocol on page 107 for more information on RIP.

The routingProtocol attribute has the following values:

Value	Description
none	No routing protocol is used. Only static routes are used.
rip	The RIP routing protocol is active. You can set the RIP version per interface. Refer to the elements txVersion and rxVersion in the rip structure (refer to 7.3.3 - Explaining the rip structure on page 110).

telindus1031/router/alternativeRoutes

Default:backup
Range: enumerated, see below

Use this attribute to determine how the Telindus 1031 Router deals with identical routes.

If more than one route to a (sub-)network is defined in the routing table, and these routes have …

- identical destination addresses, masks, preferences and metrics,
- a different gateway,

… then you can use the alternativeRoutes attribute to determine which route the Telindus 1031 Router uses to reach the (sub-)network.

The alternativeRoutes attribute has the following values:

Value	Description
backup	The Telindus 1031 Router always uses the same route to reach the (sub-)network. Only when this route goes down, it uses the alternative route.
roundRobin	The Telindus 1031 Router alternately uses the two possible routes to reach the (sub-)network. However, once a certain route is used to reach a specific address, this same route is always used to reach this specific address.

telindus1031/router/ripUpdateInterval

Default:00000d 00h 00m 30s
Range: 00000d 00h 00m 05s - 00000d 00h 10m 00s

Use this attribute to set the interval the Telindus 1031 Router transmits RIP update messages.

Normally, RIP update messages are transmitted every 30 seconds. It is possible to change this interval. However, changing this interval will also change the lifetime of routes learnt through RIP. If a RIP route is received for the last time, it is declared down after 6 times the ripUpdateInterval. After the route is down, it is deleted after 4 times the ripUpdateInterval.

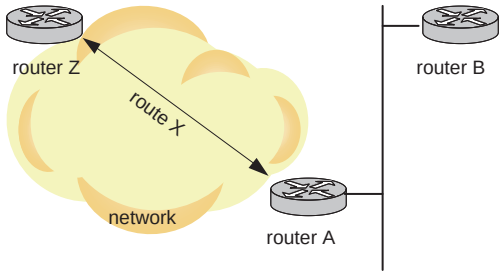
telindus1031/router/ripHoldDownTime

Default:00000d 00h 03m 00s
Range: 00000d 00h 00m 00s - 00000d 00h 10m 00s

Use this attribute to set the time the Telindus 1031 Router has to hold a route down in case it receives a RIP update message declaring this route down.

What is the RIP hold-down time?

Suppose you have a situation as depicted in the figure alongside.



Now suppose the following happens:

1. Route X goes down.
   ⇒Router A sends a RIP update message to router B declaring route X down.
2. Only a few moments later, route X goes up for a while after which it goes down again. This continues for a certain time. In other words, the route status toggles between up and down.
   ⇒Every time the status of route X changes, Router A sends a RIP update message to router B. Also router B propagates these RIP update messages. In other words, the toggling of route X causes that a lot of RIP update messages are sent.

The ripHoldDownTime attribute tries to avoid situations as described above. Suppose router B has a ripHoldDownTime attribute. In that case, the situation is as follows:

1. Route X goes down.
   ⇒Router A sends a RIP update message to router B declaring route X down. Router B starts the RIP hold-down timer.
2. The status of route X starts toggling between up and down.
   ⇒Router A sends several RIP update messages concerning route X to router B. Router B holds the status of route X down, as longs as the RIP hold-down timer has not expired.

When the RIP hold-down timer expires and the route is …

- down, then the route status stays down.
- up, then the route status changes to up.

telindus1031/router/ripv2SecretTable

Default:<empty>
Range: table, see below

Use this attribute to define the secrets used for the RIP authentication.

Refer to 7.3.4 - Configuring RIP authentication on page 115 for more information on RIP authentication.

The ripv2SecretTable table contains the following elements:

Element	Description
keyId	Use this element to set a unique identifier for each secret. Default:0 Range: 0 … 255
secret	Use this element to define the secret. Default:<empty> Range: 0 … 16 characters This secret is sent with the RIP updates on the specified interface. It is also used to authenticate incoming RIP updates.
interface	Use this element to specify on which interface the secret is used. Default:all Range: 0 … 24 characters Entering the string “all” (default) means the secret is used on all the interfaces.

Remarks

- If authentication is enabled (either text or md5), then only updates using that authentication are processed. All other updates on that interface are discarded.
- If you use md5 and if for a certain interface multiple secrets are present in the ripv2SecretTable, then the first entry in the ripv2SecretTable is used to transmit RIP updates. Authentication of the received RIP updates is done by looking for the first secret with a matching key.
- If you use text and if for a certain interface multiple secrets are present in the ripv2SecretTable, then only the first entry in the ripv2SecretTable is used to transmit and receive RIP updates.

telindus1031/router/sysSecret

Default:<empty>
Range: 0 … 64 characters

Use this attribute for the CHAP authentication process. The CHAP authenticator uses the sysSecret attribute in order to verify the peer its response.

Refer to 6.2.4 - Configuring PPP authentication on page 76 for more information on CHAP authentication.

telindus1031/router/pppSecretTable

Default:<empty>
Range: table, see below

Use this attribute for the CHAP authentication process. Enter the CHAP name and secret of the remote router in this table.

Refer to 6.2.4 - Configuring PPP authentication on page 76 for more information on CHAP authentication.

The ripv2SecretTable table contains the following elements:

Element	Description
name	Use this element to set the CHAP name of the remote router. Default:<empty> Range: 0 … 64 characters If the remote router is a Telindus 1031 Router, then the name element should correspond with the remote Telindus 1031 Router its sysName attribute.
secret	Use this element to set the CHAP secret of the remote router. Default:<empty> Range: 0 … 64 characters If the remote router is a Telindus 1031 Router, then the secret element should correspond with the remote Telindus 1031 Router its sysSecret attribute.

telindus1031/router/helperProtocols

Default:<empty>
Range: table, see below

Use this attribute to define the TCP and UDP port numbers for which broadcast forwarding is required. Use this attribute if you specified helper IP addresses using the helperAddresses element in the ip structure of the LAN interface. Refer to 5.2.3 - Explaining the ip structure on page 58.

If the helperProtocols table is empty (default), then address substitution is applied for the following protocols:

Protocol name	TCP/UDP port number
Time Server	37
IEN-116 Host Name Server	42
Domain Name Server	53
TACACS database service	65
Boot Protocol (BootP) / DHCP server	68
NetBIOS Name Server	137
NetBIOS Datagram Server	138

Important remark

Specifying at least one value in the helperProtocols table clears the default helper list automatically. In that case, if you want that for instance NetBios Datagram Server broadcast is forwarded, you have to specify port number 138 again.

For BootP / DHCP broadcast packets, the Telindus 1031 Router is also a BootP / DHCP Relay Agent. If the protocol is selected, then the Telindus 1031 Router will write the IP address of its Ethernet interface in the BootP or DHCP gateway field and increment the hops field in addition to the address substitution.

telindus1031/router/sendTtlExceeded

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “TTL exceeded“ messages.

What is Time To Live (TTL)?

Each IP packet has a Time To Live (TTL) value in its header. Each device that sends an IP packet sets this parameter at some fixed or predefined value. When the packet enters a router, the router decrements the TTL value. If a router finds a value 0 after decrementing the TTL, it discards the packet. This because a value 0 means the packet has passed too many routers. Probably the packet is looping between a number of routers. This mechanism avoids that routers with configuration errors bring down a complete network.

The ICMP message “TTL exceeded”

If a router discards a packet because its TTL is exceeded, it normally sends an ICMP “TTL exceeded“ message to the originator of the packet. With the sendTtlExceeded attribute you can define whether you want the Telindus 1031 Router to send such ICMP messages or not.

The sendTtlExceeded attribute has the following values:

Value	Description
enabled	The Telindus 1031 Router sends ICMP “TTL exceeded" messages.
disabled	The Telindus 1031 Router does not send ICMP “TTL exceeded” messages. This also implies that the router is not recognised by the UNIX or Windows traceroute feature.

telindus1031/router/sendPortUnreachable

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “Destination unreachable: Port unreachable“ messages.

The ICMP message “port unreachable”

The Telindus 1031 Router supports a number of higher-layer IP protocols (Telnet, SNMP and TMA) for management purposes. If an IP packet is sent to the Telindus 1031 Router for a higher-layer protocol that it does not support, it normally sends an ICMP “Destination unreachable: Port unreachable“ message to the originator of the packet. With the sendPortUnreachable attribute you can define whether you want the Telindus 1031 Router to send such an ICMP message or not.

The sendPortUnreachable attribute has the following values:

Value	Description
enabled	The Telindus 1031 Router sends ICMP “port unreachable" messages.
disabled	The Telindus 1031 Router does not send ICMP “port unreachable” messages. This also implies that the router is not recognised by the UNIX or Windows traceroute feature.

telindus1031/router/sendAdminUnreachable

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP "Destination unreachable: Communication with destination is administratively prohibited” messages.

The ICMP message “communication prohibited”

If the Telindus 1031 Router receives an IP packet that is destined for a prohibited destination (because this destination is defined in an access list), then it sends an ICMP "Destination unreachable: Communication with destination is administratively prohibited” message to the originator of the packet. With this attribute you can define whether you want the Telindus 1031 Router to send such an ICMP message or not.

The sendAdminUnreachable attribute has the following values:

Value	Description
enabled	The Telindus 1031 Router sends ICMP “communication prohibited“ messages.
disabled	The Telindus 1031 Router does not send ICMP “communication prohibited“ messages.

telindus1031/router/dhcpStatic

Default:<empty>
Range: table, see below

Use this attribute to assign a fixed IP address to a client its MAC address and this for an infinite time.

The Telindus 1031 Router supports the DHCP server protocol. This attribute and the following two attributes describe the configuration parameters to customise the DHCP server behaviour.

The dhcpStatic table contains the following elements:

Element	Description
ipAddress	Use this element to assign an IP address to a certain client. This client is identified with its MAC address. Default:0.0.0.0 Range: up to 255.255.255.255 If no IP address is specified, then there is no connection to the client. In that case, all other attributes in the table are ignored for this client.
mask	Use this element to set the client its subnet mask. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	Use this element to set the default gateway for the client its subnet. Default:0.0.0.0 Range: up to 255.255.255.255 If no gateway is specified, then the gateway of the LAN channel is used.
nameServer	Use this element to set the IP address of the name server that is available to the client. Default:0.0.0.0 Range: up to 255.255.255.255
tftpServer	Use this element to set the IP address of the TFTP server that is available to the client. It is the next server to use in boottrap. Default:0.0.0.0 Range: up to 255.255.255.255
macAddress	Use this element to enter the client its MAC address. Default:0.0.0.0.0.0 Range: up to ff.ff.ff.ff.ff.ff If no MAC address is specified, then there is no connection to the client. Therefore, all other attributes in the table are ignored for this client.
bootFile	Use this element to set the location of the boot file. Default:<empty> Range: max. 128 characters
hostName	Use this element to set the name of the client. Default:<empty> Range: max. 20 characters
domainName	Use this element to set the name the client should use when resolving hostnames via the Domain Name System (DNS). Default:<empty> Range: max. 20 characters
netbiosNameServer	Use this element to set the IP address of the NetBios server. Default:0.0.0.0 Range: up to 255.255.255.255
netbiosNodeType	Use this element to configure the client as described in RFC1001 / RFC1002. Default:<opt> Range: enumerated, see below The netbiosNodeType element has the following values: no-node, B-node, P-node, M-node, H-node.

telindus1031/router/dhcpDynamic

Default:<empty>
Range: table, see below

Use this attribute to specify the IP address range from which an IP address may be dynamically assigned to a client its MAC address.

The dhcpDynamic table contains the following elements:

Element	Description
ipStartAddress	Use this element to define the start address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. Default:0.0.0.0 Range: up to 255.255.255.255 If no IP start address is specified, all other attributes on the same line in the table are ignored.
ipEndAddress	Use this element to define the end address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. Default:0.0.0.0 Range: up to 255.255.255.255 The IP address range will only contain the ipStartAddress in case … • no ipEndAddress is specified, • the specified ipEndAddress is the same as the ipStartAddress, • the specified ipEndAddress is smaller than the ipStartAddress, • the specified ipEndAddress belongs to another subnet than the ipStartAddress. Do not include the Telindus 1031 Router its own IP address in this range!
mask	Use this element to set the client its subnet mask for the specified IP address range. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	Use this element to set the default gateway for the client its subnet. Default:0.0.0.0 Range: up to 255.255.255.255 If no gateway is specified, then the gateway of the LAN channel is used.
nameServer	Use this element to set the IP address of the name server that is available to the client. Default:0.0.0.0 Range: up to 255.255.255.255
tftpServer	Use this element to set the IP address of the TFTP server that is available to the client. It is the next server to use in boottrap. Default:0.0.0.0 Range: up to 255.255.255.255
leaseTime	Use this element to set the maximum time a client can lease an IP address from the specified IP address range. Default:00000d 00h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s If 00000d 00h 00m 00s (default) is specified, then the lease time is infinite.
holdTime	Use this element to set the time between two consecutive leases of an IP address. I.e. if a client has just let go of its dynamically assigned IP address, then this same IP address can not be reassigned before the holdTime has elapsed. Default:00000d 00h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Element	Description
bootFile	Use this element to set the location of the boot file. Default:<empty> Range: max. 128 characters
hostName	Use this element to set the name of the client. Default:<empty> Range: max. 20 characters Because the DHCP server can not give the same name to all clients of this IP address range, a number is added to the host name from the second IP address onwards. The number goes up to 99. **Example** Suppose the host name is Telindus. In that case the name for the start IP address is Telindus, for the second IP address Telindus1, and so on.
domainName	Use this element to set the name the client should use when resolving hostnames via the Domain Name System (DNS). Default:<empty> Range: max. 20 characters
netbiosNameServer	Use this element to set the IP address of the NetBios server. Default:0.0.0.0 Range: up to 255.255.255.255
netbiosNodeType	Use this element to configure the client as described in RFC1001 / RFC1002. Default:<opt> Range: enumerated, see below The netbiosNodeType element has the following values: no-node, B-node, P-node, M-node, H-node.

DHCP server reaction on a BootP request

The DHCP server reacts on a BootP request as follows: the source MAC address of the incoming BootP request packet is compared with the MAC addresses that have been entered in the dhcpStatic table. Then, there are two possibilities:

- If the source MAC address corresponds with a MAC address in the dhcpStatic table, then the DHCP server replies with a BootP reply packet. In this reply, the IP address that is linked with the MAC address in question (as defined in the dhcpStatic table) is returned.
- If the source MAC address does not correspond with a MAC address in the dhcpStatic table, then the DHCP server returns no response on that frame.

Releasing IP addresses - DHCP versus BootP

On DHCP level, it is regularly checked whether the device that has an IP address in lease is still connected to the network. If it is not, the IP address is returned to the pool of free IP addresses.

On BootP level, however, such a check (or *refresh*) does not exist. What is more, a statistic IP address lease is for an infinite time. Consequently, if the device that requested the IP address is no longer connected to the network, this is not detected by the server. In that case, the statistical information will still indicate that the IP address is leased although it is not.

telindus1031/router/dhcpCheckAddress

Default:disabled
Range: enabled / disabled

Use this attribute to allow that the assigned IP address is probed with an ICMP Echo Request. This checks and prevents the double use of IP addresses.

The dhcpCheckAddress attribute has the following values:

Value	Description
enabled	No ICMP Echo Request is sent when an IP address is leased by a client.
disabled	An ICMP Echo Request is sent when an IP address is leased by a client. If an ICMP Echo Reply is received, it means the IP address is already in use. Therefore, another IP address is assigned.

telindus1031/router/alarmMask

telindus1031/router/alarmLevel

Refer to …

- 13.2 - Introducing the alarm attributes on page 329 for more information on the configuration attributes alarmMask and alarmLevel and on the alarms in general.
- 13.7 - Router alarms on page 337 for more information on the alarms of the router object.

10.5.2 Default NAT configuration attributes

telindus1031/router/defaultNat/patAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to enter the official IP address that has to be used for the Port Address Translation. Entering an address different from the default value 0.0.0.0 automatically enables PAT.

Refer to 7.4 - Configuring address translation on page 116 for more information on PAT.

telindus1031/router/defaultNat/portTranslations

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges that should not be translated.

Some TCP or UDP applications do not allow port translations: these applications require a dedicated source port number. In the portTranslations table you can define UDP and TCP port ranges that should not be translated. If a packet with a source port number in such a range is received, PAT replaces only the source IP address provided it is the first device using this port number. When other devices using the same application (hence the same port number) try to send traffic to the same Internet destination address, PAT discards this traffic.

It is also possible to define port ranges that PAT should always discard. The port translation range PAT uses goes from 60928 up to 65535.

The portTranslations table contains the following elements:

Element	Description
protocol	Use this element to select the protocol: tcp or udp. Default:tcp Range: tcp / udp
startPort	Use this element to set the lowest value of the TCP or UDP port range. Default:0 Range: 0 … 65535
endPort	Use this element to set the highest value of the TCP or UDP port range. Default:<opt> Range: 0 … 65535 If no endPort value is defined (<opt>), then the port range is limited to the startPort value only.
action	Use this element to set the action in case a packet is received with a source port number that falls within the specified port range. Default:noTranslation Range: enumerated, see below The action element has the following values:

Value	Description
noTranslation	The port numbers that fall within the specified port range are not translated.
deny	Packets with port numbers that fall within the specified port range are discarded.

telindus1031/router/defaultNat/servicesAvailable

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges for incoming Internet traffic that should not be translated. Instead it is sent to the corresponding private IP address.

The servicesAvailable table makes it possible to have a server on the local network that can be accessed from the Internet, although it has no official IP address.

The servicesAvailable table contains the following elements:

Element	Description
protocol	Use this element to select the protocol: tcp or udp. Default:tcp Range: tcp / udp
startPort	Use this element to set the lowest value of the TCP or UDP port range. Default:0 Range: 0 … 65535
endPort	Use this element to set the highest value of the TCP or UDP port range. Default:<opt> Range: 0 … 65535 If no endPort value is defined (<opt>), then the port range is limited to the startPort value only.
serverAddress	Use this element to set the private server address. Default:0.0.0.0 Range: up to 255.255.255.255 If a packet is received with a source port number that falls within the specified port range, then it is sent to the private server address.

telindus1031/router/defaultNat/addresses

Default:<empty>
Range: table, see below

Use this attribute to enter all the official IP addresses that have to be used for Network Address Translation. Entering an address in the table automatically enables NAT.

The addresses table contains the following elements:

Element	Description
officialAddress	Use this element to set the official IP address. These addresses are used in the reverse order as they appear in the list.
privateAddress	Use this element to set the private IP address, i.e. to permanently assign an official IP address to a private address.

Refer to 7.4 - Configuring address translation on page 116 for more information on NAT.

telindus1031/router/defaultNat/gateway

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to define the gateway addresses from routes on which NAT or PAT should be applied.

telindus1031/router/defaultNat/tcpSocketTimeOut

Default:00001d 00h 00m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the time-out for TCP sessions that are not closed by the application.

Such sessions, whether PAT or NAT is in use, remain active for one day by default. Only decrease this attribute if some TCP applications do not close properly, filling up the available translation sessions.

telindus1031/router/defaultNat/udpSocketTimeOut

Default:00000d 00h 03m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the time-out for UDP sessions that are not closed by the application.

Such sessions, whether PAT or NAT is in use, remain active for 3 minutes by default. Only decrease this attribute if some UDP applications do not close properly, filling up the available translation sessions.

telindus1031/router/defaultNat/tcpSockets

Default:1024
Range: 500 … 4500

Use this attribute to set the maximum number of TCP session that may be used simultaneously for address translation.

telindus1031/router/defaultNat/udpSockets

Default:1024
Range: 500 … 4500

Use this attribute to set the maximum number of UDP session that may be used simultaneously for address translation.

telindus1031/router/defaultNat/dmzHost

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to set the address of the DMZ (demilitarised zone) host.

What is a DMZ host?

In computer networks, a DMZ (demilitarised zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed.

10.5.3 L2TP tunnel configuration attributes

telindus1031/router/tunnels/l2tpTunnels

Default:<empty>
Range: table, see below

Use this attribute to configure the Layer 2 Tunnelling Protocol tunnels you want to set up.

The l2tpTunnels table contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the tunnel. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate the tunnel (down). Default:down Range: up / down
mode	Use this element to determine whether for the corresponding tunnel, IP packets are treated by the routing process, the bridging process or both. Default:routing Range: enumerated, see below The mode element has the following values: **Value** / **Description** bridging: All packets received on the tunnel are bridged. routing: All packets received on the tunnel are routed. routingAndBridging: The SNAP header is checked to determine whether the packets have to be bridged or routed.
ip	Use this element to configure the IP related parameters of the tunnel. Default:- Range: structure, see below Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.
bridging	Use this element to configure the bridging related parameters of the tunnel. Default:- Range: structure, see below When bridging is enabled on a tunnel interface, the tunnel acts exactly as a bridge port for a physical PPP connection. Refer to … • 8 - Configuring the bridge on page 139 for more information on bridging. • 8.9.6 - Explaining the bridging structure on page 152 for a detailed description of the bridging structure.
l2tp	Use this element to configure the L2TP related parameters of the tunnel. Default:- Range: structure, see below Refer to telindus1031/router/tunnels/l2tpTunnels/l2tp on page 219 for a detailed description of the l2tp structure,.

telindus1031/router/tunnels/l2tpTunnels/l2tp

Default:-
Range: structure, see below

Use the l2tp structure in the l2tpTunnels table to configure the L2TP related parameters of the tunnel.

The l2tp structure contains the following elements:

Element	Description
localIpAddress	Use this element to set the official IP address that serves as start point of the L2TP connection. Default:<opt> Range: up to 255.255.255.255
remoteIpAddress	Use this element to set the official IP address that serves as end point of the L2TP connection. Default:<opt> Range: up to 255.255.255.255 Both localIpAddress and remoteIpAddress together with the well-known port number for L2TP (i.e. 1701), make up the socket used for the L2TP session. At the moment, only one L2TP session can exist between one localIpAddress and remoteIpAddress combination.
pppAuthentication	Use this element to enable or disable CHAP authentication on the PPP connection in the tunnel. Default:disabled Range: enabled / disabled Refer to telindus1031/g703[ ]/channel[ ]/ppp/authentication on page 187 for more information.
type	Use this element to specify the tunnel type. Default:outgoingDial Range: enumerated, see below The type element has the following values: **Value** / **Description** outgoingDial — The outgoing tunnel is not continuously open. It is opened whenever data has to be sent through the tunnel, and closed when no data is detected for a certain time. outgoingLeasedLine — The outgoing tunnel is opened as soon as the Telindus 1031 Router is up, and it stays open. incoming — The tunnel is an incoming tunnel.
dataChannelSequenceNumbering	Use this element to enable (on) or disable (off) sequence numbering on the data messages. These sequence numbers are used to detect lost packets and/or restore the original sequence of packets that may have been reordered during transport. Default:off Range: on / off On control messages, sequence numbering is always enabled. It is recommended that for connections where reordering or packet loss may occur, dataChannelSequenceNumbering is enabled.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>keepAliveTimeOut</td><td>Use this element to set the amount of time (in seconds) the tunnel waits before it sends a keep alive message in case it receives no data.
Default:30
Range: 1 … 3600

If the tunnel does not receive incoming data during a certain time, it sends a keep alive message to the other side and waits for an acknowledgement.</td></tr>
<tr><td>l2tpMode</td><td>Use this element to set the L2TP function of the Telindus 1031 Router.

The l2tpMode element has the following values:

<table><tr><th>Value</th><th>Description</th></tr><tr><td>lac</td><td>The Telindus 1031 Router acts as an L2TP Access Concentrator.</td></tr><tr><td>lns</td><td>The Telindus 1031 Router acts as an L2TP Network Server</td></tr><tr><td>auto</td><td>If both local and remote Telindus 1031 Router are set to auto, they mutually decide who will be the LAC and who the LNS.</td></tr></table>
Select auto only if you use a Telindus router at both sides of the tunnel. In conjunction with routers from other vendors (e.g. Cisco), specifically select an L2TP mode (lac or lns).</td></tr>
<tr><td>tunnelAuthentication</td><td>Use this element to enable (on) or disable (off) tunnel authentication.
Default:off
Range: on / off

L2TP incorporates a simple, optional, CHAP-like tunnel authentication system during control connection establishment.

If the LAC or LNS wishes to authenticate the identity of the peer it is contacting or being contacted by, it sends a challenge packet. If the expected response and response received from a peer does not match, the tunnel is not opened.

To participate in tunnel authentication, a single shared secret has to exist between the LAC and LNS.</td></tr>
<tr><td>tunnelSecret</td><td>Use this element to set the tunnel secret. This secret is used in the tunnel authentication in order to verify the peer its response.
Default:<empty>
Range: 0 … 64 characters</td></tr>
<tr><td>copyTos</td><td>Use this element to enable (on) or disable (off) the copying of the Type Of Service (TOS) field value of the packets.
Default:on
Range: on / off</td></tr>
<tr><td>maxNrOfRetransmissions</td><td>Use this element to set the number of times a control message has to be retransmitted in case no acknowledgement follows, before the tunnel is closed.
Default:4
Range: 0 … 10</td></tr>
</table>

Element	Description
transmitWindowSize	Use this element to set the window size for transmitting control messages. Default:4 Range: 1 … 30
receiveWindowSize	Use this element to set the window size for receiving control messages. Default:4 Range: 1 … 30
udpChecksum	Use this element to enable (on) or disable (off) the UDP checksum. Default:off Range: on / off It is recommended to enable the UDP checksum on lower quality links.

10.5.4 Routing filter configuration attributes

The routingFilter object is not present in the containment tree by default. If you want to use a routing filter, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.

telindus1031/router/routingFilter[ ]/filter

Default:<empty>
Range: table, see below

Use this attribute to set up a RIP update filter.

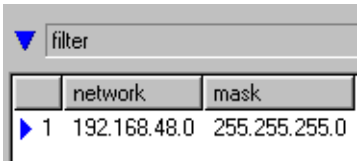
RIP updates coming from a network that is specified in the filter table are forwarded. All other RIP updates are blocked. If the filter table is empty, then all RIP updates are forwarded.

The filter table contains the following elements:

Element	Description
network	This is the IP source address of the RIP update. The address may be a (sub)network address. Default:0.0.0.0 Range: up to 255.255.255.255
mask	This is the IP subnet mask for the network. By combining an IP address with a mask you can uniquely identify a range of addresses. Default:255.255.255.0 Range: up to 255.255.255.255

Example

This example shows a filter that only forwards RIP updates coming from subnet 192.168.48.0.



10.5.5 Traffic policy configuration attributes

The trafficPolicy object is not present in the containment tree by default. If you want to use traffic policy, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.

telindus1031/router/trafficPolicy[ ]/method

Default:trafficShaping
Range: enumerated, see below

Use this attribute to choose, on traffic overload conditions, how and which queues are filled with the “excess” data.

The method attribute has the following values:

Value	Description
trafficShaping	The data is redirected to the queues based on the settings of the attribute telindus1031/router/trafficPolicy[ ]/trafficShaping. Note that the traffic shaping can be used for more than queuing alone. It can also be used to set up an extended access list.
tosDiffServ	The data is redirected to the queues based on *DiffServ* (refer to RFC2597) regarding class and drop precedence. This means that, depending on their Type Of Service (TOS) field, some packets are moved to other queues and/or dropped sooner than other packets in case the queue is full. The highest 3 bits of the TOS field are mapped as follows: **Bit values … / are mapped to …** 000 up to 100 / queues 1 up to 5, respectively. 101 and higher / the low delay queue. The next 2 bits define the drop levels: **Bit values … / correspond with …** 00 and 01 / maxLength1 10 / maxLength2 11 / maxLength3 Refer to the attribute telindus1031/router/trafficPolicy[ ]/dropLevels for more information on drop levels.
tosMapped	The data is redirected to the queues based on the settings of the attribute telindus1031/router/trafficPolicy[ ]/tos2QueueMapping.

telindus1031/router/trafficPolicy[ ]/trafficShaping

Default:<empty>
Range: table, see below

The function of this attribute is twofold:

- In case you have set the telindus1031/router/trafficPolicy[ ]/method attribute to trafficShaping, then use the trafficShaping table to specify which data has to be redirected to which queue.
  If an overload condition occurs, then a packet is redirected to the specified queue when the criteria as specified in the trafficShaping table are met.
- You can use the trafficShaping table to set up an extended access list.
  A packet is forwarded if the criteria as specified in the trafficShaping table are met. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range.
  The extended access list itself is activated by specifying the trafficPolicy object its index name in a trafficPolicy attribute of a certain interface. For example in the ip structure of the …
  - lanInterface object,
  - pvcTable,
  - etcetera.

The trafficShaping table contains the following elements:

Element	Description
sourceIpStart-Address	Use these elements to set the IP source address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
sourceIpEnd-Address	Packets that fall within the specified range are forwarded and queued if applicable.
destinationIpStart-Address	Use these elements to set the IP destination address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
destinationIpEnd-Address	Packets that fall within the specified range are forwarded and queued if applicable.
tosStartValue	Use these elements to set the Type Of Service field value. Default:any(start)/optional(end) Range: 0 … 256
tosEndtValue	Packets that fall within the specified range are forwarded and queued if applicable.
ipProtocol	Use this element to set the protocol field from the IP header. Default:any Range: 0 … 255 Packets that have the specified protocol field are forwarded and queued if applicable. You can specify the protocol by typing the protocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).

Element	Description
sourcePortStart sourcePortEnd	Use these elements to set the source port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 Packets that fall within the specified range are forwarded and queued if applicable. You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).
destinationPortStart destinationPortEnd	Use these elements to set the destination port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 Packets that fall within the specified range are forwarded and queued if applicable. You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.
newTosValue	Use this element to set the new TOS field value. Default:unchanged Range: 0 … 256 When you select a new TOS field value, then a packet that matches an entry in the trafficShaping table its TOS field value is changed. Selecting unchanged, leaves the TOS field value as it is.
priority	Use this element to set the destination queue for a packet matching an entry in the trafficShaping table. Default:Queue1 Range: enumerated, see below In case an overload condition occurs, then a packet that matches an entry in the trafficShaping table is sent to the specified queue. The priority element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

Start and end values

Except for the ipProtocol, newTosValue and priority elements, it is possible to specify ranges using the start and end values. There are two special cases:

- A start value is entered, but no end value ⇒ an exact match is needed for the start value.
- Neither a start nor an end value is entered ⇒ the field is not checked.

telindus1031/router/trafficPolicy[ ]/dropLevels

Default:-
Range: table, see below

Use this attribute to define for each user configurable queue, how many packets may be queued before they are dropped.

The dropLevels table contains the following elements:

Element	Description
maxLength1	This is the maximum length / drop level 1. Default:100 Range: 1 … 3000 In case you set the attribute telindus1031/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then only this drop level is relevant. • tosDiffServ, then this drop level corresponds with the drop level bits value 00 and 01.
maxLength2	This is the maximum length / drop level 2. Default:100 Range: 1 … 3000 In case you set the attribute telindus1031/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop level bits value 10.
maxLength3	This is the maximum length / drop level 3. Default:100 Range: 1 … 3000 In case you set the attribute telindus1031/router/trafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop level bits value 11.

Examples

Suppose …

- telindus1031/router/trafficPolicy[ ]/method is set to trafficShaping or tosMapped.
- for queue 1 you set maxLength1 = 1000, for queue 2 to 500, for queue 3 to 3000, for queue 4 to 1000 and for queue 5 to 200.

In this case, packets are dropped when the amount of packets in the queue exceeds the amount as specified with the maxLength1 element.

Suppose …

- telindus1031/router/trafficPolicy[ ]/method is set to tosDiffServ.
- for queue 1 you set maxLength1 = 100, maxLength2 = 200 and maxLength3 = 50.

In this case, the following applies:

Queue 1 contains … data packets.	An incoming data packet with … is …		
	drop level[1] 1	drop level 2	drop level 3
less than 50	accepted	accepted	accepted
more than 50, less than 100	accepted	accepted	dropped
more than 100, less than 200	dropped	accepted	dropped
more than 200	dropped	dropped	dropped

1. As defined in the TOS field.

telindus1031/router/trafficPolicy[ ]/tos2QueueMapping

Default:<empty>
Range: table, see below

In case you have set the telindus1031/router/trafficPolicy[ ]/method attribute to tosMapped, then use the tos2QueueMapping table to specify which data has to be redirected to which queue.

The tos2QueueMapping table contains the following elements:

Element	Description
startTos endTos	Use these elements to set the Type Of Service field value. Default:0 (start) / 255 (end) Range: 0 … 255 Packets that have a Type Of Service field value within the specified range are redirected to the targetQueue.
targetQueue	Use this element to set the destination queue. Default:Queue1 Range: enumerated, see below The targetQueue element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue.

10.5.6 Priority policy configuration attributes

The priorityPolicy object is not present in the containment tree by default. If you want to use priority policy, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.

telindus1031/router/priorityPolicy[ ]/algorithm

Default:fifo
Range: enumerated, see below

Use this attribute to determine how and which queues are emptied.

The algorithm attribute has the following values:

Value	Description
fifo	This is a First In First Out queue. The data that enters the queue first, also leaves the queue first. This is the fastest but most superficial queuing mechanism.
roundRobin	This is a priority queuing mechanism. In this case, all user configurable queues containing data have an equal weight. In other words, if all the user configurable queues contain data, they are addressed in turns. However the low delay queue and system queue still have priority over the user configurable queues:

Queue	Priority
1 - 5 : user configurable queue	These queues are addressed in turns.
6 : low delay queue	This queue is addressed between every user configurable queue.
7 : system queue	This queue has priority over all other queues. As soon as it contains data, it is emptied.

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>absolutePriority</td><td>This is a priority queuing mechanism. In this case, queues with a high priority have absolute priority over queues with a low priority. In other words, no lower priority queue is emptied as long as a higher priority queue contains data.

The priority of the queues runs parallel to the queue number. I.e. the user configurable queue number 1 has the lowest priority, whereas the system queue (number 7) has the highest priority:

<table>
<tr><th>Queue</th><th>Priority</th></tr>
<tr><td>1 - 5 : user configurable queue</td><td>Queue 1 has the lowest priority whereas queue 5 has the highest priority. A lower priority queue is only emptied in case no higher priority queue contains data.</td></tr>
<tr><td>6 : low delay queue</td><td>This queue is only emptied in case the system queue contains no data.</td></tr>
<tr><td>7 : system queue</td><td>This queue has priority over all other queues. As soon as it contains data, it is emptied.</td></tr>
</table>

Note that there is a risk of starvation. This means that it is possible that the lower priority queues are never emptied because a higher priority queue continuously receives data.</td></tr>
<tr><td>weightedFair-Queueing</td><td>This is a priority queuing mechanism. In this case, the user configurable queues are addressed based on their weight. However the low delay queue and system queue still have priority over the user configurable queues:

<table>
<tr><th>Queue</th><th>Priority</th></tr>
<tr><td>1 - 5 : user configurable queue</td><td>These queues are addressed based on their weight. The weight can be configured in the telindus1031/router/priorityPolicy[ ]/queueConfigurations attribute.</td></tr>
<tr><td>6 : low delay queue</td><td>This queue is addressed between every user configurable queue.</td></tr>
<tr><td>7 : system queue</td><td>This queue has priority over all other queues. As soon as it contains data, it is emptied.</td></tr>
</table>
</td></tr>
</table>

telindus1031/router/priorityPolicy[ ]/countingPolicy

Default:bytes
Range: enumerated, see below

Use this attribute to define whether the quotum of the queues is expressed in bytes or packets.

telindus1031/router/priorityPolicy[ ]/queueConfigurations

Default:<empty>
Range: table, see below

Use this attribute to …

- set the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed.
- set the relative importance of the user configurable queues.

The queueConfigurations table contains the following elements:

Element	Description
quotum	Use this element to set the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed. Default:1500 Range: 1 … 25000 The unit of the quotum (bytes or packets) can be set with the telindus1031/router/priorityPolicy[ ]/countingPolicy attribute.
weight	Use this element to set the relative importance of the user configurable queues. Default:1 Range: 1 … 10 The weight element is only relevant in case the telindus1031/router/priorityPolicy[ ]/algorithm attribute is set to weightedFairQueueing. **Example** Suppose queue 1 has weight 2, queue 2 has weight 1 and both queues contain data. In that case the queues are emptied in the following order: queue 1 → queue 1 → queue 2 → queue 1 → queue 1 → queue 2 → etc.

telindus1031/router/priorityPolicy[ ]/lowdelayQuotum

Default:1500
Range: 1 … 25000

Use this attribute to set the number of bytes/packets that is dequeued from the low delay queue when the queue is addressed. The unit of the quotum (bytes or packets) can be set with the telindus1031/router/priorityPolicy[ ]/countingPolicy attribute.

Refer to 7.6.1 - Introducing traffic and priority policy on page 131 for more information on queues.

10.6 Bridge configuration attributes

This section discusses the configuration attributes concerned with bridging. First it describes the general bridging configuration attributes. Then it explains the configuration attributes of the extra features as there are access listing, user priority mapping, etc…

The following gives an overview of this section:

- 10.6.1 - Bridge group configuration attributes on page 232
- 10.6.2 - Bridge access list configuration attributes on page 236
- 10.6.3 - Bridge traffic policy configuration attributes on page 237

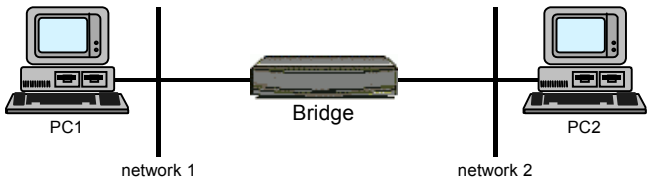
10.6.1 Bridge group configuration attributes

telindus1031/bridge/bridgeGroup/bridgeCache

Default:learning
Range: learning / disabled

Use this attribute to enable or disable the “filter” functionality of the bridge.

The bridgeCache attribute has the following values:

Value	Description
learning	The bridge acts as a filter. Data coming from network 1, will only be let through by the bridge if this data has a destination outside network 1 or if it has a broadcast or multicast address. This means the bridge filters the data and decreases the amount of data traffic on the separated LAN segments. 
disabled	The bridge acts as a repeater. All the data which originates from network 1 will be let through to network 2. Even if the data is not destined for that network.

What is the bridge cache?

Whereas the ARP cache keeps MAC address - IP address pairs, the bridge cache (also called address database) keeps MAC address - interface pairs. This allows the bridge to know which device is reachable through which interface. Refer to telindus1031/bridge/bridgeGroup/bridgeCache on page 289 for an example of such a table.

telindus1031/bridge/bridgeGroup/bridgeTimeOut

Default:00000d 00h 05m 00s
Range: 00000d 00h 00m 00s-
24855d 03h 14m 07s

Use this attribute to set the ageing time of the bridge cache entries.

The bridge cache time-out

If devices on the network are (re)moved then the MAC address - interface relation changes (refer to What is the bridge cache?). Therefore, the bridge cache entries are automatically removed from the cache after a fixed time-out. This time-out period can be set with the bridgeTimeOut attribute. This in case no topology change is detected, otherwise the time-out is equal to the value of the bridgeForwardDelay element of the spanningTree attribute.

When checking the bridgeCache it may appear that some entries are present for a longer time than is configured with the bridgeTimeOut attribute. This because the entries in the bridgeCache are not monitored continuously, but once per minute. As a result, some entries may appear to be “overtime”. However, this should be no more than ± 75 seconds.

telindus1031/bridge/bridgeGroup/name

Default:bridge
Range: 1 … 24 characters

Use this attribute to assign an administrative name to the bridge.

telindus1031/bridge/bridgeGroup/ip

Default:<empty>
Range: structure, see below

Use this attribute to configure the IP related parameters of the bridge.

Important remark

If you set the configuration attribute telindus1031/lanInterface/mode to bridging, then the settings of the configuration attribute telindus1031/lanInterface/ip are ignored. As a result, if you want to manage the Telindus 1031 Router via IP, you have to configure an IP address in the bridgeGroup object instead: telindus1031/bridge/bridgeGroup/ip.

Refer to 5.2.3 - Explaining the ip structure on page 58 for a detailed description of the ip structure.

telindus1031/bridge/bridgeGroup/arp

Default:-
Range: structure, see below

Use this attribute to configure the Address Resolution Protocol (ARP) cache of the bridge.

Refer to telindus1031/lanInterface/arp on page 179 for a detailed description of the arp structure.

telindus1031/bridge/bridgeGroup/spanningTree

Default:-
Range: structure, see below

Use this attribute to configure the bridging related parameters.

Whereas the bridging attribute groups the bridging related parameters per interface, the spanningTree attribute groups the bridging related parameters of the bridge as a whole.

The spanningTree structure contains the following elements:

Element	Description
protocol	Use this element to select the bridging protocol. Default:none Range: enumerated, see below The protocol element has the following values: **Value** / **Description** none: The Telindus 1031 Router uses the self-learning principle. This means that the bridge itself learns which data it has to forward and which data it has to block. I.e. it builds its own bridging table. p802.1D: The Telindus 1031 Router uses the self-learning principle in conjunction with the Spanning Tree protocol. Because Spanning Tree bridging is somewhat more complicated than self-learning bridging, an introduction is given in 8.2 - The self-learning and Transparent Spanning Tree bridge on page 141. When using Frame Relay or ATM encapsulation on the WAN interface together with the Spanning Tree protocol, every DLCI or PVC link is considered as a separate bridge port. Each link is than considered as a special kind of LAN with only both end points connected.
bridgePriority	Use this element to set the priority of the bridge. Default:32768 Range: 0 ... 65535 The bridge its MAC address together with the bridgePriority element form a unique bridge identifier. This identifier is used to determine which bridge becomes the root bridge. The bridge with the lowest bridgePriority value becomes the root bridge. If two bridges have the same bridgePriority value, then the bridge with the lowest MAC address becomes the root bridge.
bridgeMaxAge	Use this element to set the time the bridge retains bridging information before discarding it. Default:00000d 00h 00m 20s Range: 00000d 00h 00m 06s - 00000d 00h 00m 40s
bridgeHelloTime	Use this element to set the interval by which the root bridge sends Configuration BPDUs, also called Hello messages. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 01s - 00000d 00h 00m 10s

Element	Description
bridgeForwardDelay	Use this element to set … Default:00000d 00h 00m 15s Range: 00000d 00h 00m 04s - 00000d 00h 00m 30s • the delay a bridge port applies to move from listening state to learning state or from learning state to forwarding state. Refer to 8.5 - The Spanning Tree bridge port states on page 144 for more information on the possible states of a bridge port. • the time-out (or ageing) for purging MAC addresses from the bridge cache in case a topology change is detected.

telindus1031/bridge/bridgeGroup/vlan

Default:-
Range: structure, see below

Use this attribute to configure some VLAN parameters.

Although the Telindus 1031 Router bridges IEEE 802.1Q tagged frames when connected to a VLAN aware switch, the Telindus 1031 Router itself can only be managed via IP if some VLAN parameters are configured.

The vlan structure contains the following elements:

Element	Description
dotQTagging	Use this element to enable or disable … Default:disabled Range: enabled / disabled • the 802.1Q tagging of Ethernet frames sent by the Telindus 1031 Router. • the recognition of 802.1Q tagged frames received by the Telindus 1031 Router.
vid	Use this element to set the ID of the VLAN over which the Telindus 1031 Router can be managed. Default:1 Range: 1 … 4094
userPriority	Use this element to set the priority used in the 802.1p part of the 802.1Q header and this for all frames sent by the Telindus 1031 Router. Default:0 Range: 0 … 7

If dotQTagging is enabled, then the Telindus 1031 Router does not interpret spanning tree frames but just forwards them. In that case the spanning tree protocol should be disabled on the Telindus 1031 Router.

10.6.2 Bridge access list configuration attributes

The accessList object is not present in the containment tree by default. If you want to use a bridge access list, then add this object first. Refer to 4.4 - Adding an object to the containment tree on page 45.

telindus1031/bridge/accessList[ ]/macAddress

Default:<empty>
Range: table, see below

Use this attribute to filter bridged frames based on the source MAC address.

The access list is applied on the transmitted (outgoing) data of the interface. Packets coming from MAC addresses that are specified in the access list are not sent out on the interface on which the access list is applied.

10.6.3 Bridge traffic policy configuration attributes

telindus1031/bridge/trafficPolicy/vlanPriorityMap

Default:-
Range: structure, see below

Use this attribute to impose a traffic policy on the bridged (VLAN) frames received by the Telindus 1031 Router.

Each VLAN frame has a certain priority (this is specified in the 802.1p part of the 802.1Q header of the VLAN frame). In case a traffic overload condition occurs and in case you imposed this traffic policy on a certain interface, then the VLAN frames are sent to a queue. Using the vlanPriorityMap attribute, you can specify which VLAN frame is sent to which queue based on the priority of the VLAN frame.

The vlanPriorityMap structure contains the following elements:

Element	Description
priority0 … priority7	Use these elements to define which priority corresponds with which queue. The possible queues are: queue1 up to queue5 and lowDelayQueue. To empty these queues, specify a priority policy. Frames that are not tagged are all considered to have priority 0. Refer to 8.10 - Configuring traffic and priority policy on the bridge on page 154 for more information on traffic policy, priority policy and priority queuing.

10.7 SNMP configuration attributes

telindus1031/snmp/trapDestinations

Default:<empty>
Range: table, see below

Use this attribute to define to which IP address the SNMP traps have to be sent.

The Telindus 1031 Router translates all alarm status changes into SNMP traps. These traps can then be sent to a management system. To enable this, configure in the trapDestinations table the IP addresses to which the traps have to be sent. If the trapDestinations table is empty then no traps are sent.

The trapDestinations table contains the following elements:

Element	Description
address	Use this element to set the IP address of the management station to which the SNMP trap messages have to be sent. Default:0.0.0.0 Range: up to 255.255.255.255
community	Use this element to set the community string which is included in the SNMP traps that are sent to the management station. It is used as a password in the SNMP communication. Give it the same value as on your SNMP management station. Default:public Range: 0 … 20 characters

telindus1031/snmp/mib2Traps

Default:off
Range: on / off

Use this attribute to enable (on) or disable (off) the sending of SNMP traps as MIB2 traps.

If you want to send the SNMP traps as MIB2 traps, proceed as follows:

Step	Action
1	Select the trapDestinations attribute. Add an entry to this table for each network management station that should receive SNMP traps.
2	In the trapDestinations table, define the IP address of the management stations that should receive the SNMP traps.
3	In the trapDestinations table, configure the community element associated with each trap destination.
4	Configure the mib2Traps attribute: **Value** / **Description** on: Select this value if the management station is any SNMP station (without the TMA for HP OpenView application). In that case, the Telindus 1031 Router sends the alarms coldBoot, warmBoot and linkDown as MIB2 traps instead of enterprise specific (private) MIB traps. off: Select this value if the management system is the TMA for HP OpenView application. In that case the Telindus 1031 Router sends all alarms as enterprise specific (private) MIB traps.
5	Set for each object of the Telindus 1031 Router: • the alarms that you want to send using the attribute alarmMask. • the importance of each alarm using the attribute alarmLevel. By default only the most important alarms are enabled.

10.8 Management configuration attributes

telindus1031/management/cms2Address

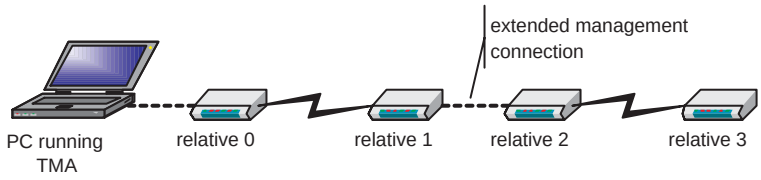
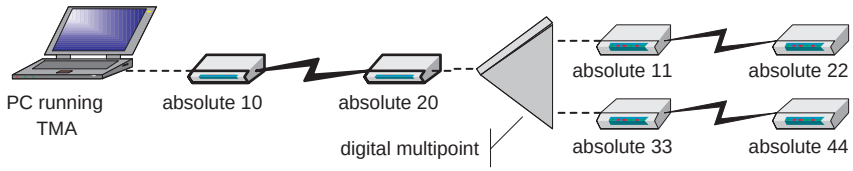
Default:0
Range: 0 … 65535

Use this attribute to assign an absolute address to the Telindus 1031 Router.

What is relative and absolute addressing?

If you want to connect with TMA to a Telindus device, you have to specify the address of the device in the *Connect…* window. Refer to 4 - Managing the Telindus 1031 Router on page 33.

There are two different address types: relative and absolute. The following table explains the difference between these address types:

Type	Description
relative	This type of addressing is meant for a network topology where the Telindus devices are connected in-line on management level. I.e. with extended management connections between two Telindus devices. An extended management connection is realised with a crossed cable between the control connectors of two Telindus devices.  To enable relative addressing, no address has to be specified in the Telindus device.
absolute	This type of addressing is meant for a network topology where the Telindus devices are not connected in-line on management level. I.e. when there is a digital multipoint device present.  To enable absolute addressing, an address has to be specified in the Telindus device. Do this with the cms2Address attribute.

telindus1031/management/accessList

Default:<empty>
Range: table, see below

Use this attribute to control the access from certain hosts or networks.

The access list filters incoming traffic, based on the source IP address. You can specify multiple entries within the access list. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range. If not one entry matches, then the packet is dropped. If the access list is empty, then all packets are forwarded.

The accessList table contains the following elements:

Element	Description
sourceAddress	Use this element to set the IP source address of the packet. The address may be a (sub)network address. Default:0.0.0.0 Range: up to 255.255.255.255
mask	Use this element to set the IP subnet mask for the sourceAddress. By combining an IP address with a mask you can uniquely identify a range of addresses. Default:255.255.255.255 Range: up to 255.255.255.255
action	Use this element to set the action when a packet arrives with a source IP address that falls within the specified address range. Default:deny Range: enumerated, see below The possible actions are: **Value** / **Description** deny / The packet is dropped. allow / The packet is forwarded.

If you specify one entry or multiple entries for which the action is set to deny, then also specify at least one entry for which the action is set to allow. Else all packets are dropped!

Example 1

This example shows an access list that only allows traffic from subnet 192.168.48.0, except for packets from station 192.168.48.10.

accessList

	sourceAddress	mask	action
1	192.168.48.0	255.255.255.0	allow
2	192.168.48.10	255.255.255.255	deny

Example 2

The next example shows an access list that allows all traffic, except the traffic from subnet 192.168.48.0. The second entry is the rule to add if you want all packets that do not match the previous entries to be allowed.

accessList

	sourceAddress	mask	action
1	192.168.48.0	255.255.255.0	deny
2	0.0.0.0	0.0.0.0	allow

telindus1031/management/snmp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enable) or discard (disable) SNMP requests.

telindus1031/management/telnet

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enable) or discard (disable) Telnet sessions.

Use this attribute also to accept (enable) or discard (disable) HTTP (Web Interface) sessions.

telindus1031/management/tftp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enable) or discard (disable) TFTP sessions.

telindus1031/management/consoleNoTrafficTimeOut

Default:00000d 00h 30m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to set the time-out period after which a management session is closed when there is no user interaction.

The purpose of such a timer is to protect the Telindus 1031 Router against unauthorised access in case the last user did not close his session.

telindus1031/management/ctrlPortProtocol

Default:console
Range: enumerated, see below

Use this attribute to set the function of the control connector.

The ctrlPortProtocol attribute has the following values:

Value	Description
management	Select this value if you want to connect the control connector of the Telindus 1031 Router to … • a management concentrator for management purposes. • the control connector of another Telindus 1031 Router using a crossed cable (i.e. they are connected back-to-back) in order to create an extended management link. Refer to What is relative and absolute addressing? on page 240 for more information on extended management links. When connecting the control connector of the Telindus 1031 Router to a COM port of your computer, you can still open a TMA session on the Telindus 1031 Router. You can however not open a CLI or ATWIN session.
console	Select this value if you want to connect the control connector of the Telindus 1031 Router to a COM port of your computer in order to manage the Telindus 1031 Router using TMA, CLI, ATWIN, etc.

telindus1031/management/alarmFilter

Default:0
Range: 0 … 50000

Use this attribute to selectively ignore / drop alarms in TMA for HP OpenView if these alarms are below a certain level.

The filter number that you define using the alarmFilter attribute, has to correspond with a filter that you have to define in the Alarm Manager of TMA for HP OpenView. In the Alarm Manager, it is possible to specify a minimum alarm level that is needed before alarms are logged in HP OpenView. This can be specified for each filter number.

Loop-back configuration attributes

telindus1031/management/loopback/ipAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to assign an IP address to the loop-back interface.

The loop-back interface is a software interface which can be used for management purposes. This interface is always up, regardless of the state of the physical interfaces. This means the router will always respond to ICMP echo requests sent to this address. In every other respect the loop-back address behaves the same as an IP address of a physical interface.

If the loop-back address is used and RIP is active, then a host route to the loop-back address is included in the RIP updates.

10.9 Proxy configuration attributes

Refer to the Telindus 1030 Router Orchid function manual for more information on the configuration attributes of the proxy function (also called Orchid function).

11 Status attributes

This chapter discusses the status attributes of the Telindus 1031 Router. The following gives an overview of this chapter:

- 11.1 - Status attribute overview on page 246
- 11.2 - General status attributes on page 248
- 11.3 - LAN interface status attributes on page 251
- 11.4 - WAN interface status attributes on page 257
- 11.5 - Router status attributes on page 273
- 11.6 - Bridge status attributes on page 287
- 11.7 - Management status attributes on page 293
- 11.8 - File system status attributes on page 294
- 11.9 - Operating system status attributes on page 296
- 11.10 - Proxy status attributes on page 297

11.1 Status attribute overview

> telindus1031
- sysDescr
- sysObjectID
- sysUpTime
- sysServices
- flash1Version
- flash2Version
- activeFlash
- flashVersions
- bootVersion
- loaderVersion
- messages
- deviceId
- configurationSaving

>> lanInterface
- ifDescr
- ifType
- ifOperStatus
- ifLastChange
- ifSpeed
- ifMtu
- ip
- macAddress
- arpCache
- bridging
- adapter
- ipAdEntBcastAddr
- ipAdEntReasmMaxSize
- Action: clearArpCache

>> g703[1]
- ifDescr
- ifType
- ifOperStatus
- ifSpeed
- coding
- los
- lfa
- ais
- openCircuit
- rxLevel

>>> channel[g703_1]
- ifDescr
- ifType
- ifOperStatus
- ifLastChange
- ifSpeed
- ifMtu

>>>> ppp
- ip
- lcpState
- ipcpState
- bcpState
- lcpMyOptions
- lcpHisOptions
- ipcpMyOptions
- ipcpHisOptions
- bcpMyOptions
- bcpHisOptions
- myAuthenState
- hisAuthenState
- bridging

>>>> frameRelay
- ip
- dlciTable
- lmi
- cllmLastCongestionCause

>>>> atm
- atmSync
- pvcTable

>>>> hdlc
- bridging

>> router
- routingTable
- igmpTable
- dhcpBinding
- dhcpStatistics

>>> defaultNat
- addresses

>>> tunnels
- l2tpTunnels

>> bridge

>>> bridgeGroup
ifDescr
ifType
ifOperStatus
ifMtu
ip
arpCache
bridgeCache
bridging
spanningTree
Action: clearArpCache
Action: clearBridgeCache

>> management
cms2Address

>>> loopback
ifDescr
ifType
ifOperStatus
ifMtu
ipAddress

>> fileSystem
fileList
freeSpace
status
corruptBlocks
Action: Delete File
Action: Rename File

>> operatingSystem
taskInfo

>> proxy
Refer to the Telindus 1030 Router Orchid function manual for more information on the status attributes of the proxy function (also called Orchid function).

11.2 General status attributes

telindus1031/sysDescr

This attribute displays a textual description of the device. It is an SNMP MIB2 parameter.

Example: Telindus 1031 Router Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Telindus 1031 Router is the device name.
- Txxxx/xxxxx is the application software code and version.
- 01/01/00 12:00 is the application software release date and time.

telindus1031/sysObjectID

This attribute displays the identification string. This is an SNMP MIB2 parameter.

telindus1031/sysUpTime

This attribute displays the elapsed time since the last power-on or cold boot of the Telindus 1031 Router. This is an SNMP MIB2 parameter.

telindus1031/sysServices

This attribute displays the service identification. This is an SNMP MIB2 parameter.

telindus1031/flash1Version

This attribute displays the code and version of the application software stored as CONTROL1.

Example: Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Txxxx is the application software code for this device.
- /xxxxx is the application software version.
- 01/01/00 is the application software release date.
- 12:00 is the application software release time.

telindus1031/flash2Version

This attribute displays the code and version of the application software stored as CONTROL2.

telindus1031/activeFlash

This attribute displays which application software is currently active. Possible values are:

Value	Description
flash1	The application software CONTROL1 is active.
flash2	The application software CONTROL2 is active.

telindus1031/flashVersions

This attribute displays how many application software versions can be stored in the file system.

telindus1031/bootVersion

This attribute displays the code, version, release date and time of the boot software currently used in the Telindus 1031 Router.

telindus1031/loaderVersion

This attribute displays the code, version, release date and time of the loader software currently used in the Telindus 1031 Router.

telindus1031/messages

This attribute displays informative and error messages, e.g. Reconfigured, Cold Boot, … The messages table displays maximum 20 messages.

If you open a TMA session on the Telindus 1031 Router over IP, i.e. not through the control port, then the messages are also sent to the control port. This means that if you open a terminal emulation session on the control port, you can monitor these messages. If you hit the ENTER key, the messages stop and you get the (CLI) password prompt.

telindus1031/deviceId

This attribute displays a unique code. This code is programmed into the Telindus 1031 Router before it leaves the factory. You can use this code for inventory purposes.

telindus1031/configurationSaving

This attribute indicates when the Telindus 1031 Router is writing its (new) configuration to the flash memory. Possible values are:

Value	Description
busy	The Telindus 1031 Router is busy writing its configuration to the flash memory. During this state, do not power-down or reboot the Telindus 1031 Router else the new configuration will be lost.
done	The Telindus 1031 Router has finished writing its configuration to the flash memory.

11.3 LAN interface status attributes

telindus1031/lanInterface/ifDescr

This attribute displays the interface description. This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifType

This attribute displays the interface type. This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOperStatus

This attribute displays the current operational status of the interface. This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifLastChange

This attribute shows the system-up time on the moment the interface entered its current operational state. I.e. the moment the value of the ifOperStatus status attribute changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status attribute.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifSpeed

This attribute displays the interface speed in bits per second (bps). This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ip

This attribute displays the IP information of the interface.

The ip structure contains the following elements:

Element	Description
status	This is the current operational status of the IP layer (layer 3).
address	This is the IP address of the interface. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the interface. It is either configured or retrieved automatically.

telindus1031/lanInterface/macAddress

This attribute displays the MAC address of the Telindus 1031 Router its LAN interface.

The LAN interface has been allocated a fixed Ethernet address, also called MAC (Medium Access Control) address. The MAC address is globally unique and can not be modified. It is a 6 byte code, represented in hexadecimal format. Each byte in the code is separated by a colon.

Refer to What is the ARP cache? on page 179 for more information on the MAC addresses.

telindus1031/lanInterface/arpCache

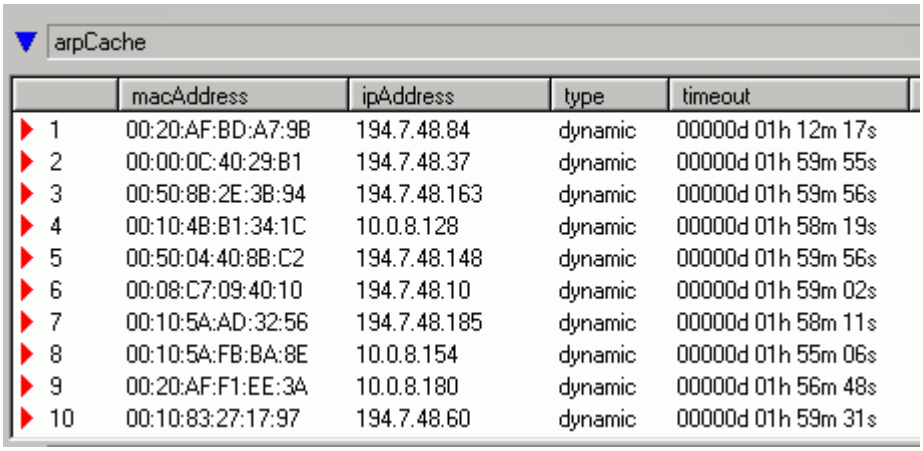
This attribute displays all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface. Refer to What is the ARP cache? on page 179 for more information.

The arpCache table contains the following elements:

Element	Description
macAddress	This is the MAC address.
ipAddress	This is the associated IP address.
type	This is the ARP cache entry type. Possible values are: **Value** / **Description** dynamic: The MAC - IP address pair is retrieved from an ARP request or reply message. static: The MAC - IP address pair is configured. There is only one static entry, i.e. the Telindus 1031 Router its own IP and MAC address.
timeOut	This is the time the entry will remain in the ARP cache. For the static entry, this value is 0.

Example

The following figure shows part of an ARP cache table as an example:



	macAddress	ipAddress	type	timeout
1	00:20:AF:BD:A7:9B	194.7.48.84	dynamic	00000d 01h 12m 17s
2	00:00:0C:40:29:B1	194.7.48.37	dynamic	00000d 01h 59m 55s
3	00:50:8B:2E:3B:94	194.7.48.163	dynamic	00000d 01h 59m 56s
4	00:10:4B:B1:34:1C	10.0.8.128	dynamic	00000d 01h 58m 19s
5	00:50:04:40:8B:C2	194.7.48.148	dynamic	00000d 01h 59m 56s
6	00:08:C7:09:40:10	194.7.48.10	dynamic	00000d 01h 59m 02s
7	00:10:5A:AD:32:56	194.7.48.185	dynamic	00000d 01h 58m 11s
8	00:10:5A:FB:BA:8E	10.0.8.154	dynamic	00000d 01h 55m 06s
9	00:20:AF:F1:EE:3A	10.0.8.180	dynamic	00000d 01h 56m 48s
10	00:10:83:27:17:97	194.7.48.60	dynamic	00000d 01h 59m 31s

telindus1031/lanInterface/bridging

This attribute displays the bridging status of the interface.

The bridging structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>state</td><td>This displays the current state of the port. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled *</td><td>The port is not in use because of a management action.</td></tr>
<tr><td>blocking</td><td>The port does not participate in frame forwarding.</td></tr>
<tr><td>listening</td><td>The port prepares to participate in frame forwarding, but it does not update its MAC address database (also called bridge cache).</td></tr>
<tr><td>learning</td><td>The port prepares to participate in frame forwarding, and it learns the present MAC addresses.</td></tr>
<tr><td>forwarding *</td><td>The port participates in frame forwarding.</td></tr>
</table>
* These are the only possible port states for a bridge that is not running the Spanning Tree protocol (IEEE p802.1D).

Refer to 8.5 - The Spanning Tree bridge port states on page 144 for more information on port states.[1]</td></tr>
<tr><td>subState[1]</td><td>This gives additional information on the port state. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>root</td><td>This is the port through which the root bridge can be reached. Consequently, the root bridge itself does not have a root port. All other bridges must have a root port.</td></tr>
<tr><td>designated</td><td>This is the designated port for this (virtual) LAN. All ports of the root bridge are designated ports.</td></tr>
<tr><td>alternate</td><td>This port is not active. Either because of a management action, or through protocol intervention.</td></tr>
</table></td></tr>
</table>

Element	Description
designatedPriority[1]	Together, these two elements form a unique bridge identifier. Depending whether the current port is a designated port or not, these two elements display the unique bridge identifier of … • the bridge to which this port belongs, in case of a designated port. • the bridge believed to be the designated bridge for the LAN that is currently connected to this port, in all other cases. This bridge identifier is used … • together with the designatedPortPriority and designatedPortId attributes to determine whether this port should be the designated port for the LAN that is currently connected to this port. • to test the value of the bridge identifier parameter conveyed in received Configuration BPDUs.
designatedMac[1]	
designatedPort-Priority[1]	Together, these two elements form a unique port identifier. They display the unique port identifier of the bridge port through which the designated bridge transmits the configuration message information stored by this port. This port identifier is used … • together with the designatedPriority and designatedMac attributes to determine whether this port should be the designated port for the LAN that is currently connected to this port. • by the management system to determine the topology of the bridged LAN.
designatedPortId[1]	
topologyChangeAck[1]	This displays the value of the Topology Change Acknowledgement flag in the next Configuration BPDU that will be transmitted on this port. This element is used to assess the need to set the Topology Change Acknowledgement flag in response to a received Topology Change Notification BPDU.
configuration-Pending[1]	This is used to determine whether a Configuration BPDU should be transmitted on this port after expiry of the hold timer. This avoids that Configuration BPDUs are transmitted too often, although ensuring that up-to-date information is transmitted.

1. Only relevant when the bridge uses the Spanning Tree Protocol.

telindus1031/lanInterface/adapter

This attribute displays the Ethernet mode of the LAN interface as set using the telindus1031/lanInterface/adapter attribute.

The adapter structure contains the following elements:

Element	Description
speed	This is the Ethernet speed. Possible values are: 10 and 100.
duplex	This is the Ethernet duplex mode. Possible values are: halfDuplex and fullDuplex.

telindus1031/lanInterface/ipAdEntBcastAddr

This attribute displays the value of the least-significant bit in the IP broadcast address. This address is used for sending packets on the interface which is associated with the IP address of this entry. The value applies to the general broadcast, the subnet and network broadcasts.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ipAdEntReasmMaxSize

This attribute displays the size of the largest IP packet which this entity can re-assemble from incoming IP fragmented packets received on this interface.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/clearArpCache

If you execute this action, the ARP cache table is cleared.

11.4 WAN interface status attributes

This section discusses the status attributes of the WAN interface. First it describes the status attributes of the physical interface. Then it explains the status attributes of the encapsulation protocols that can be used on the interface.

The following gives an overview of this section:

- 11.4.1 - G703 interface status attributes on page 258
- 11.4.2 - G703 channel status attributes on page 259
- 11.4.3 - PPP status attributes on page 261
- 11.4.4 - Frame Relay status attributes on page 266
- 11.4.5 - ATM status attributes on page 270
- 11.4.6 - HDLC status attributes on page 272

11.4.1 G703 interface status attributes

telindus1031/g703[ ]/ifDescr

This attribute displays the interface description. This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/ifType

This attribute displays the interface type. This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/ifOperStatus

This attribute displays the current operational status of the interface. This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/ifSpeed

This attribute displays the interface speed in bits per second (bps). This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/coding

This attribute displays which G.703 encoding mode is currently in use (ami or hdb3). Refer to telindus1031/g703[ ]/coding on page 182 for more information on the encoding modes.

telindus1031/g703[ ]/los

This attribute displays (on / off) whether a Loss Of Signal has been detected. LOS is on when the incoming data is no longer present. E.g. the connection *from* the WAN *towards* the Telindus 1031 Router is interrupted.

telindus1031/g703[ ]/lfa

This attribute displays (on / off) whether a Loss of Frame Alignment has been detected. LFA is on when the Frame Alignment Signal (FAS), which is present in time slot 0 of the G.704 framed data, is not detected after a certain period.

telindus1031/g703[ ]/ais

This attribute displays (on / off) whether an Alarm Indication Signal has been detected. AIS is on when the AIS signal (also called *all ones*) is detected on the incoming data. E.g. a device / application in the network detected a problem and communicates this to the other devices in the network.

telindus1031/g703[ ]/openCircuit

This attribute displays (on / off) whether the transmit side is connected or not. Open circuit is on when e.g. the connection *from* the Telindus 1031 Router *towards* the WAN is interrupted.

telindus1031/g703[ ]/rxLevel

This attribute displays the signal level, in dB, of the incoming data.

11.4.2 G703 channel status attributes

telindus1031/g703[ ]/channel[ ]/ifDescr

This attribute displays the interface description. This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/channel[ ]/ifType

This attribute displays the interface type. This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/channel[ ]/ifLastChange

This attribute shows the system-up time on the moment the interface entered its current operational state. I.e. the moment the value of the ifOperStatus status attribute changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status attribute.

This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/channel[ ]/ifSpeed

This attribute displays the interface speed in bits per second (bps). This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/channel[ ]/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface.

This is an SNMP MIB2 parameter.

telindus1031/g703[ ]/channel[ ]/ifOperStatus

This attribute displays the current operational status of the interface. This is an SNMP MIB2 parameter.

Possible values are:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>up</td><td>The WAN interface is up, data transfer is possible.
The following table shows you in which case the value of the ifOperStatus attribute is up:
<table>
<tr><th>Protocol</th><th>The ifOperStatus attribute is up (i.e. the alarm wanInterface/alarmInfo/linkDown = off) in case …</th></tr>
<tr><td>Frame Relay</td><td>• LMI is up.
• the bit pump is synchronised.</td></tr>
<tr><td>PPP</td><td>• LCP is open.
• the bit pump is synchronised.</td></tr>
<tr><td>ATM</td><td>• the PVC is truly up.
• the bit pump is synchronised.</td></tr>
</table></td></tr>
<tr><td>down</td><td>The WAN interface is down, data transfer is not possible.</td></tr>
</table>

Important remarks

- Whether the Telindus 1031 Router is configured in bridging or routing has no effect on the value of the attributes telindus1031/wanInterface/ifOperStatus:Status and telindus1031/wanInterface/alarmInfo/linkDown:Alarms.
- In case of Frame Relay, if the configuration element telindus1031/wanInterface/frameRelay/lmi/auto is set to noLmi, then the value of the status element telindus1031/wanInterface/frameRelay/lmi/status:Status is always up. However, the other conditions as stated in the table above remain.
- In case of PPP, if the configuration element telindus1031/wanInterface/ppp/linkMonitoring/operation is set to disabled, then it is possible that the wanInterface/ifOperStatus value does not go down even if the link quality is too bad for a proper data link. This because the link monitoring mechanism is the only PPP mechanism that will start a renegotiation of the LCP layer.
- In case of ATM, if the configuration element telindus1031/wanInterface/atm/pvcTable/atm/oamF5Loopback is set to disabled, then the ifOperStatus of the PVC becomes up when the ATM is synchronised globally. However, this does not guarantee that the PVC is configured (correctly) on the remote side. However, the other conditions as stated in the table above remain.

11.4.3 PPP status attributes

telindus1031/g703[ ]/channel[ ]/ppp/ip

This attribute displays the IP information of the PPP link.

The ip structure contains the following elements:

Element	Description
status	This is the current operational status of the IP layer (layer 3) of the PPP link.
address	This is the IP address of the PPP link. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the PPP link. It is either configured or retrieved automatically.
remote	This is the IP address of the remote end of the PPP link. It is either configured or retrieved automatically.

telindus1031/g703[ ]/channel[ ]/ppp/lcpState

This attribute reflects the status of the LCP (Link Control Protocol) protocol. Possible values are:

Value	Description
Initial	LCP handshake has not started yet.
Starting, Closed, Stopped, Closing, Stopping	These values correspond with the transient states in the LCP state diagram.
Req-Sent	The local side of the PPP link has sent an LCP request. The remote side did not answer yet.
Ack-Rcvd	The local side of the PPP link has received an LCP acknowledge from the remote side. This is a transient state.
Ack-Sent	The local side of the PPP link has acknowledged the LCP request from the remote side.
Opened	The LCP handshake succeeded.

telindus1031/g703[ ]/channel[ ]/ppp/ipcpState

This attribute reflects the status of the IPCP (Internet Protocol Control Protocol) protocol. The possible values are the same as those of telindus1031/g703[ ]/channel[ ]/ppp/lcpState.

telindus1031/g703[ ]/channel[ ]/ppp/bcpState

This attribute reflects the status of the BCP (Bridging Control Protocol) protocol. The possible values are the same as those of telindus1031/g703[ ]/channel[ ]/ppp/lcpState.

telindus1031/g703[ ]/channel[ ]/ppp/lcpMyOptions

During the LCP handshake, a number of options can be exchanged between the local and remote side of the link. This attribute lists the LCP options for the router at this side (local side) of the link.

The lcpMyOptions table contains the following elements:

Element	Description
option	The Telindus 1031 Router supports the following LCP options: **Value** / **Description** 3 — This is the Authentication-Protocol option. 5 — This is the Magic-Number option. For more information on the LCP configuration options, refer to RFC1661.
length	This is the length of the option field.
value	This is the option value represented as an octet string (hexadecimal ASCII representation).

telindus1031/g703[ ]/channel[ ]/ppp/lcpHisOptions

This attribute lists the LCP options for the router at the other side (remote side) of the link. The lcpMyOptions table contains the same elements as the telindus1031/g703[ ]/channel[ ]/ppp/lcpMyOptions table.

Other option values than the ones supported by the Telindus 1031 Router may be present.

telindus1031/g703[ ]/channel[ ]/ppp/ipcpMyOptions

During the IPCP handshake, a number of options can be exchanged between the local and remote side of the link. This attribute lists the IPCP options for the router at this side (local side) of the link.

The ipcpMyOptions table contains the following elements:

Element	Description
option	The Telindus 1031 Router supports the following IPCP option: • 3 : the IP-Address option. For more information on the IPCP configuration options, refer to RFC1332.
length	This is the length of the option field.
value	This is the option value represented as an octet string (hexadecimal ASCII representation).

telindus1031/g703[ ]/channel[ ]/ppp/ipcpHisOptions

This attribute lists the IPCP options for the router at the other side (remote side) of the link. The ipcpHisOptions table contains the same elements as the telindus1031/g703[ ]/channel[ ]/ppp/ipcpMyOptions table.

Other option values than the ones supported by the Telindus 1031 Router may be present.

telindus1031/g703[ ]/channel[ ]/ppp/bcpMyOptions

During the BCP handshake, a number of options can be exchanged between the local and remote side of the link. This attribute lists the BCP options for the router at this side (local side) of the link.

The bcpMyOptions table contains the following elements:

Element	Description
option	The Telindus 1031 Router supports the following LCP options: **Value** / **Description** 1 – This is the Bridge-Identification option. 2 – This is the Line-Identification option. 3 – This is the MAC-Support option. 4 – This is the Tinygram-Compression option. 5 – This is the LAN-Identification option. 6 – This is the MAC-Address option. 7 – This is the Spanning-Tree-Protocol option. For more information on the LCP configuration options, refer to RFC2878.
length	This is the length of the option field.
value	This is the option value represented as an octet string (hexadecimal ASCII representation).

telindus1031/g703[ ]/channel[ ]/ppp/bcpHisOptions

This attribute lists the BCP options for the router at the other side (remote side) of the link. The bcpMyOptions table contains the same elements as the telindus1031/g703[ ]/channel[ ]/ppp/bcpMyOptions table.

Other option values than the ones supported by the Telindus 1031 Router may be present.

telindus1031/g703[ ]/channel[ ]/ppp/myAuthenstate

This attribute displays the authentication state of the router at this side (local side) of the link. I.e. the state of the authenticator. Possible values are:

Value	Description
No-Authentication	The local side does not request PPP authentication or still has to start the CHAP authentication (LCP handshake is busy).
Wait-On-Response	The local side has sent a challenge packet and is waiting for an answer.
Authen-Successful	The response packet is found to be correct. This is the state when authentication succeeded.
Authen-Failure	The response packet is found to be incorrect. This is a transient state since the router starts the LCP handshake again after a failing authentication.

telindus1031/g703[ ]/channel[ ]/ppp/hisAuthenstate

This attribute displays the authentication state of the router at the other side (remote side) of the link. I.e. the state of the peer. Possible values are:

Value	Description
No-Authentication	This is the start-up state.
Wait-On-Challenge	During the LCP handshake the authenticator already indicates it wants to authenticate. From that moment on, the peer awaits a challenge packet.
Wait-On-Success	Once the peer has sent a response, it awaits a success or failure message.
Authen-Successful	The peer has received a success packet. It remains in this state during data transfer.
Authen-Failure	The peer has received a failure packet. This is a transient state since the router starts the LCP handshake again after a failing authentication.
Authen-Not-Allowed	This state only occurs when the peer does not accept the authentication request during the LCP handshake. A possible reason might be that the peer router does not support CHAP.

telindus1031/g703[ ]/channel[ ]/ppp/bridging

This attribute displays the bridging status of the PPP link.

Refer to telindus1031/lanInterface/bridging on page 254 for a detailed description of the bridging structure.

11.4.4 Frame Relay status attributes

telindus1031/g703[ ]/channel[ ]/frameRelay/ip

This attribute displays the IP information of the Frame Relay link.

Refer to telindus1031/lanInterface/ip on page 252 for a detailed description of the ip structure.

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable

This attribute gives the complete status information of all known DLCIs.

The dlciTable table contains the following elements:

Element	Description
name	This is the name of the DLCI as you configured it. If you did not configure a name, then this element displays: <WAN interface name> “dlci” <dlci number>. E.g. wan dlci 16
ifOperStatus	This is the current operational status of the DLCI.
ifLastChange	This is the system-up time on the moment the DLCI entered its current operational state. I.e. the moment the value of the ifOperStatus element changes (from up to down or vice versa), the system-up time value is written into the ifLastChange element.
ip	This displays the IP information of the DLCI. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/ip on page 267 for a detailed description of the ip structure.
bridging	This displays the bridging information of the DLCI. Refer to telindus1031/lanInterface/bridging on page 254 for a detailed description of the bridging structure.
frameRelay	This displays the specific Frame Relay related status information of the DLCI. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay on page 267 for a detailed description of the frameRelay structure.

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/ip

The ip structure in the dlciTable displays the IP information of the DLCI.

The ip structure contains the following elements:

Element	Description
address	This is the IP address of the DLCI. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the DLCI. It is either configured or retrieved automatically.
remote	This is the IP address of the remote end of the DLCI. It is either configured or retrieved automatically.

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay

The frameRelay structure in the dlciTable displays the specific Frame Relay related status information of the DLCI.

The frameRelay structure contains the following elements:

Element	Description
dlci	This is the DLCI identification number.
active	This indicates whether the corresponding DLCI is active (on) or not (off).
new	This is set to on if the DLCI has just been created, else it is off.
deleted	This is set to on if the DLCI has been deleted, else it is off.
rr	This element is only relevant for LMI revision 1. It is the flow control flag. If it is on, then no traffic can be sent on this DLCI. Else it is off.
bandwidth	This is the available bandwidth on this DLCI as it is communicated by the Frame Relay network.
cllmLastCongestion-Cause	CLLM (Consolidated Link Layer Management) is a Frame Relay protocol used for traffic management. The cllmLastCongestionCause element indicates the last reason, which was received from the network, for congestion on the corresponding DLCI. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/cllmLastCongestionCause on page 269 for the possible values of the cllmLastCongestionCause element.

telindus1031/g703[ ]/channel[ ]/frameRelay/lmi

This attribute gives a complete LMI status information overview.

The lmi structure contains the following elements:

Element	Description
mode	This displays the Frame Relay mode. Possible values are: noLmi, user, network, auto. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/lmi on page 191 for more information on these values.
type	This displays the LMI variant. Possible values are: lmiRev1, ansiT1-617-d, q933-Annex-A, frf1-2. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/lmi on page 191 for more information on these values.
status	This displays the current state of LMI. Possible values are: **Value** / **Description** up / LMI messages can and are exchanged. down / No LMI messages can be exchanged.
lastStatusChange	This is the system-up time when the LMI status entered its current state. I.e. the moment the value of the status element changes (from up to down or vice versa), the system-up time value is written into the lastStatusChange element.
lastError	This displays the last error condition reported by LMI. Possible values are: none, protocol error, unknown information element, sequence error, unknown report, timer expired, invalid report type, unsolicited status.
netTxSeqNum	This is the sequence number of the last LMI response frame sent towards the network.
netRxSeqNum	This is the sequence number of the last LMI command frame received from the network.
netErrors	This is the number of errors on LMI commands issued by the network during the last monitoredEvents period.
userTxSeqNum	This is the sequence number of the last LMI command frame sent towards the router.
userRxSeqNum	This is the sequence number of the last LMI response frame received from the router.

Element	Description
userErrors	This is the number of errors on LMI commands issued by the router during the last monitoredEvents period.
userWaitFullEnquiry	This is the number of LMI frames still to be sent before a Full Status Enquiry will be requested.
userLastReport-TypeSent	This displays the type of the most recent report that was sent. Possible values are: **Value** / **Description** full status — The last report contained the full status. link integrity — The last report only contained the link integrity information.

telindus1031/g703[ ]/channel[ ]/frameRelay/cllmLastCongestionCause

This attribute indicates the last reason, which was received from the network, for congestion on any of the DLCIs. Possible values are:

- none
- short term, excessive traffic
- long term, excessive traffic
- short term, equipment failure
- long term, equipment failure
- short term, maintenance action
- long term, maintenance action
- short term, unknown cause
- long term, unknown cause
- unknown cause

11.4.5 ATM status attributes

telindus1031/g703[ ]/channel[ ]/atm/atmSync

This attribute displays the ATM synchronisation status. Possible values are: synced, notSynced.

telindus1031/g703[ ]/channel[ ]/atm/pvcTable

This attribute gives the complete status information of all known PVCs.

The pvcTable table contains the following elements:

Element	Description
name	This is the name of the PVC as you configured it. If you did not configure a name, then this element displays: <WAN interface name> “vci” <vci number>. E.g. wan vci 40
ifOperStatus	This is the current operational status of the PVC.
ifLastChange	This is the system-up time on the moment the PVC entered its current operational state. I.e. the moment the value of the ifOperStatus element changes (from up to down or vice versa), the system-up time value is written into the ifLastChange element.
ip	This displays the IP information of the PVC. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/ip on page 267 for a detailed description of the ip structure.
bridging	This displays the bridging information of the PVC. Refer to telindus1031/lanInterface/bridging on page 254 for a detailed description of the bridging structure.
atm	This displays the specific ATM related status information of the PVC. Refer to telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm on page 271 for a detailed description of the atm structure

telindus1031/g703[ ]/channel[ ]/atm/pvcTable/atm

The atm structure in the pvcTable displays the specific ATM related status information of the PVC.

The atm structure contains the following elements:

Element	Description
vpi	This displays the Virtual Path Identifier (VPI) of the PVC.
vci	This displays the Virtual Channel Identifier (VCI) of the PVC. The VPI in conjunction with the VCI identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
ppp	This displays the PPP information of the PVC. For a detailed description of the elements in the ppp structure, refer to … • telindus1031/g703[ ]/channel[ ]/ppp/lcpState on page 261 • telindus1031/g703[ ]/channel[ ]/ppp/ipcpState on page 261 • telindus1031/g703[ ]/channel[ ]/ppp/bcpState on page 261 • telindus1031/g703[ ]/channel[ ]/ppp/myAuthenstate on page 265 • telindus1031/g703[ ]/channel[ ]/ppp/hisAuthenstate on page 265

11.4.6 HDLC status attributes

telindus1031/g703[ ]/channel[ ]/hdlc/bridging

This attribute displays the bridging status of the HDLC link.

Refer to telindus1031/lanInterface/bridging on page 254 for a detailed description of the bridging structure.

11.5 Router status attributes

This section discusses the status attributes concerned with routing. First it describes the general routing status attributes. Then it explains the status attributes of the extra features as there are default NAT, L2TP tunnelling, etc…

The following gives an overview of this section:

- 11.5.1 - General router status attributes on page 274
- 11.5.2 - Default NAT status attributes on page 280
- 11.5.3 - L2TP tunnel status attributes on page 281

11.5.1 General router status attributes

telindus1031/router/routingTable

This attribute lists all known routes with their operating status.

The routingTable contains the following elements:

Element	Description
network	This is the IP address of the destination network.
mask	This is the network mask of the destination network.
gateway	This is the IP address of the next router on the path to the destination network.
interface	This is the interface through which the destination network can be reached. Possible values are: **Value** / **Description** internal: The own protocol stack is used. <name>: The destination network can be reached through this particular interface. The <name> of the interface is the name as you configured it. Note that the "interface" can also be a DLCI, an ATM PVC, a tunnel, etc. discard: Packets for this destination are discarded.
encapsulation	This is the used encapsulation. It is related to the interface for this route. Possible values are: **Value** / **Description** none: The IP packets are not encapsulated. ethernet: The IP packets are encapsulated with the ARPA MAC header. frameRelay: The IP packets are encapsulated in Frame Relay (RFC1490). ppp: The IP packets are encapsulated in PPP. atm: The IP packets are encapsulated in ATM.
status	This is the route status. Possible values are: **Value** / **Description** up: The route can be used. down: The route is currently not in use. discard: Packets for this destination are discarded.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>preference</td><td>This displays the route preference. If more than one route matches the IP destination address, this attribute determines which route is used. The route with the lowest preference value will be used.</td></tr>
<tr><td>type</td><td>This is the type of the route. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>host</td><td>This is a host route, i.e. a route to a single IP address instead of a complete network. This is also used for the router its own IP address.</td></tr>
<tr><td>internal</td><td>A route with this status is irrelevant.</td></tr>
<tr><td>local</td><td>This route is for directly connected networks.</td></tr>
<tr><td>rip</td><td>This route has been received by a RIP update.</td></tr>
<tr><td>static</td><td>This route has been configured, i.e. it is a static route.</td></tr>
</table>
</td></tr>
<tr><td>metric</td><td>If two routes exist with the same preference, then the route with the lowest metric value is chosen. The metric attribute serves as a cost for using the route. In most cases it indicates the number of hops (= routers) required to reach a destination.</td></tr>
<tr><td>timeOut</td><td>In case of a RIP route, the timeOut attribute displays the time the route will remain in the routing table if no RIP updates are received anymore. For other routes this attribute always displays 00000d 00h 00m 00s.</td></tr>
</table>

Example

The following figure displays the routing table for the example in 9.1 - LAN extension over a PDH/SDH network on page 160:

routingTable

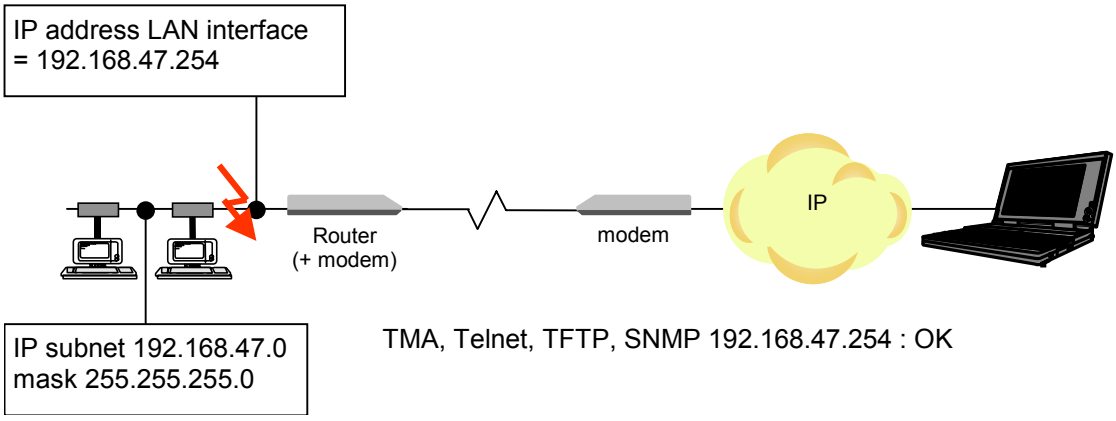
	network	mask	gateway	interface	encapsulation	status	preference	type	metric	timeout
1	0.0.0.0	0.0.0.0	127.0.0.1	discard	none	discard	255	internal	0	00000d 00h 00m 00s
2	192.168.47.0	255.255.255.0	192.168.47.254	lan	ethernet	up	1	local	1	00000d 00h 00m 00s
3	192.168.47.254	255.255.255.255	127.0.0.1	internal	none	up	1	host	0	00000d 00h 00m 00s
4	224.0.0.9	255.255.255.255	127.0.0.1	internal	none	up	1	host	0	00000d 00h 00m 00s
5	192.168.100.0	255.255.255.0	192.168.100.1	wan	ppp	down	1	local	1	00000d 00h 00m 00s
6	192.168.100.1	255.255.255.255	127.0.0.1	internal	none	down	1	host	0	00000d 00h 00m 00s
7	192.168.48.0	255.255.255.0	192.168.100.2	wan	ppp	down	10	static	1	00000d 00h 00m 00s

The lines in the routing table depicted above represent the following:

- Line 1 represents the default gateway, which is not defined.
- Lines 2 and 5 represent the subnets on the LAN and WAN interface respectively.
- Lines 3 and 6 represent the interface its IP addresses.
- Line 7 represents the static route to the remote LAN.
- Finally, line 4 represents the multicast address for RIP version 2.

Remark

If the LAN is not connected to the Telindus 1031 Router, it is still possible to contact the Telindus 1031 Router with e.g. TMA or Telnet over the WAN link by using the IP address of the LAN interface. This means that the status attribute telindus1031/lanInterface/ip/status still indicates up, although in the routingTable the corresponding route to the network is down. This seemingly unlogic implementation is necessary to insure correct operation with HP OpenView.



telindus1031/router/igmpTable

This attribute shows the multicast address, reported by one or more clients. The igmpTable is always updated, even if no proxy is configured.

The igmpTable contains the following elements:

Element	Description
multicast	This is the multicast address.
interface	This is the interface name of the client(s). In case of multiple interface names, they are separated from each other by a comma.

What is IGMP?

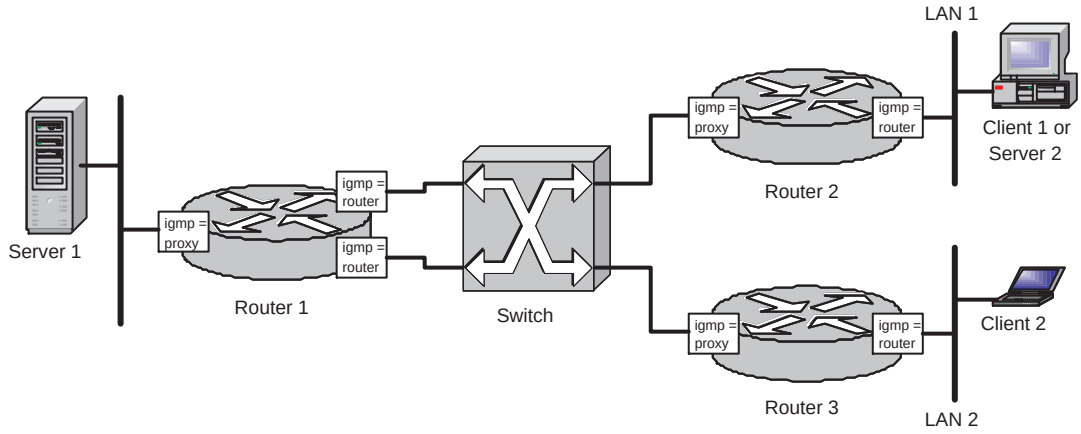
Internet Group Management Protocol (IGMP) is defined in RFC1112 as the standard for IP multicasting in the Internet.

It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group.

All hosts conforming to level 2 of the IP multicasting specification require IGMP.

IGMP topology

Consider the following multicasting topology:



In this topology …

- Client 1 and Client 2 are multicast clients.
- Router 1, 2 and 3 are multicast enabled routers.
- Server 1 is a multicast server.
- Switch is a Frame Relay or ATM switch.

The following are some characteristics of an IGMP topology:

- An IGMP router queries an IGMP proxy.
- Only 1 IGMP proxy can be defined per device.
- The TTL of an IGMP frame is always 1. IGMP messages are never forwarded.
- An IGMP frame contains an IP router alert option.
- IGMPv1 routers may be present in the network.

The multicasting IGMP protocol can be configured on every IP interface. Refer to the igmp element in 5.2.3 - Explaining the ip structure on page 58.

A client can leave or join a multicast group by erasing or adding a multicast address from a table, defined in the client application. A list of multicast group addresses is maintained in the routers. The reported multicast addresses can be seen in the igmpTable. Refer to telindus1031/router/igmpTable on page 277.

Multicast frames are always forwarded on the proxy interface. Therefore, in the IGMP topology example, it is also possible to add a multicast server (Server 2) on LAN 1. Client 2 can join a multicast group of Server S2.

Since IGMP is send in UDP (join/leave can be lost), the clients (proxies) are polled every 125 seconds:

- A general query is send to 224.0.0.1 (poll all systems).
- A leave group message is send to 224.0.0.2 (all routers).

telindus1031/router/dhcpBinding

This attribute contains a list of dynamically assigned (i.e. leased) IP addresses.

The dhcpBinding table contains the following elements:

Element	Description
ipAddress	This is the IP address that is dynamically assigned to a client.
macAddress	This is the MAC address of the client.
leaseTime	This is the remaining lease time.

telindus1031/router/dhcpStatistics

This attribute contains the statistics of all IP address ranges that have been specified in the configuration attribute telindus1031/router/dhcpDynamic.

The dhcpStatistics table contains the following elements:

Element	Description
startRange	Displays the IP start address of an IP address range.
endRange	Displays the IP end address of an IP address range.
free	For the corresponding IP address range, this displays the number of IP addresses that are still free.
lease	For the corresponding IP address range, this displays the number of IP addresses that are leased.
hold	For the corresponding IP address range, this displays the number of IP addresses that are on hold.

During power-down of the DHCP server, some leased IP addresses can still be active. Because the duration of the power-down can not be known, all timer information about lease and hold time becomes meaningless. Therefore, the DHCP server incorporated in the Telindus 1031 Router sends a ping to all leased addresses after a warm boot. When the client responds to this ping, the DHCP server resets all timers to their default value and keeps the lease with this client.

11.5.2 Default NAT status attributes

telindus1031/router/defaultNat/addresses

This attribute displays the status of each official IP address that is configured in the configuration attribute telindus1031/router/defaultNat/addresses.

The addresses table contains the following elements:

Element	Description
officialAddress	This is the official IP address as you entered it in the addresses configuration attribute.
privateAddress	This is the private IP address that is currently linked with the official IP address.
status	This is the status of the official IP address. Possible values are: **Value** / **Description** free — This official IP address is currently not in use. fixed — This address has a pre-configured mapping between the official and private IP address. allocated — This official IP address is currently assigned to a private IP address, but it is not fixed.
uses	This indicates how many sessions are currently used by this official IP address. If the attribute value becomes zero, the assigned official IP address becomes free again and can be assigned to another private IP address.

11.5.3 L2TP tunnel status attributes

telindus1031/router/tunnels/l2tpTunnels

This attribute gives you status information on the L2TP tunnels.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel as you configured it.
ifOperStatus	This displays the operational status of the tunnel. Possible values are: **Value** / **Description** up — The tunnel is up, data transfer is possible. down — The tunnel is down, data transfer is not possible. dormant — The tunnel is "stand-by". As soon as data has to be sent over the tunnel, control connect messages are exchanged and the operational status of the tunnel becomes up.
ifLastChange	This is the system-up time on the moment the tunnel entered its current operational state. I.e. the moment the value of the ifOperStatus status element changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status element.
ip	This displays the IP information of the tunnel. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/ip on page 267 for a detailed description of the ip structure.
bridging	This displays the bridging information of the tunnel. Refer to telindus1031/lanInterface/bridging on page 254 for a detailed description of the bridging structure.
l2tp	This displays the specific L2TP related status information of the tunnel. Refer to the telindus1031/router/tunnels/l2tpTunnels/l2tp on page 282 for a detailed description of the l2tp structure.
ppp	This displays the PPP information of the tunnel. For a detailed description of the elements in the ppp structure, refer to … • telindus1031/g703[ ]/channel[ ]/ppp/lcpState on page 261 • telindus1031/g703[ ]/channel[ ]/ppp/ipcpState on page 261 • telindus1031/g703[ ]/channel[ ]/ppp/bcpState on page 261 • telindus1031/g703[ ]/channel[ ]/ppp/myAuthenstate on page 265 • telindus1031/g703[ ]/channel[ ]/ppp/hisAuthenstate on page 265

telindus1031/router/tunnels/l2tpTunnels/l2tp

The l2tp structure in the l2tpTunnels table displays the specific L2TP related status information of the tunnel.

The l2tp structure contains the following elements:

Element	Description
sendingSeqNum	In case sequence numbering on the data messages is enabled (dataChannelSequenceNumbering = on), then this displays the transmit data sequence numbers.
receivingSeqNum	In case sequence numbering on the data messages is enabled (dataChannelSequenceNumbering = on), then this displays the receive data sequence numbers.
l2tpType	This displays which L2TP server type the Telindus 1031 Router currently is: LAC or LNS. If you set the configuration attribute l2tpMode to auto, then the status attribute l2tpType displays the auto value until the Telindus 1031 Routers have mutually decided who will be the LAC and who the LNS.
controlState	This displays the states associated with the LNS or LAC control connection establishment. Refer to L2TP status - control states on page 283 for more information.
callState	This displays the states associated with the LNS or LAC incoming or outgoing calls. Refer to L2TP status - call states on page 284 for more information.
deliveryState	This displays the states associated with the LNS or LAC packet delivery. Refer to L2TP status - delivery states on page 285 for more information.
authenState	This displays the states associated with the LNS or LAC authentication. Refer to L2TP status - authentication states on page 286 for more information.

L2TP status - control states

The states associated with the LNS or LAC for control connection establishment are:

Value	Description
idle	No control connection is present. Both initiator and recipient start from this state. An initiator transmits a Start Control Connection Request, while a recipient remains in the idle state until receiving a Start Control Connection Request.
waitCtlReply	This is the state where a Start Control Connection Reply is awaited.
waitCtlConn	This is the state where a Start Control Connection Connected is awaited. Upon receipt, the challenge response is checked. The tunnel either is established, or is torn down if an authorisation failure is detected.
established	The control connection is established. An established connection may be terminated by either a local condition or the receipt of a Stop Control Connection Notification. The session then returns to the idle state.

L2TP status - call states

The states associated with the LNS or LAC incoming or outgoing calls are:

Value	Description
idle	No data is exchanged over the tunnel.
waitTunnel	This is the state in which is waited … • either for the control connection to be opened, • or for verification that the tunnel is already open. Once an indication is received that the tunnel has/was opened, session control messages may be exchanged. The first of these is the Incoming Call Request.
waitReply	This is the state where an Incoming or Outgoing Call Reply message is awaited. If an Incoming or Outgoing Call Reply message is received, an incoming or Outgoing Call Connected message is sent and the session moves to the established state.
waitConnect	This is the state where an Incoming or Outgoing Call Connected message is awaited. If an Incoming or Outgoing Call Connected message is received, the call was successful and the session moves to the established state.
established	Data is exchanged over the tunnel. The session is terminated when receiving or sending a Call Disconnect Notify message. The session then returns to the idle state.

L2TP status - delivery states

The states associated with the packet delivery are:

Value	Description
operating	The Telindus 1031 Router has sent a packet, but has not received an acknowledgement on this packet yet.
idle	All transmitted packets have been acknowledged.

L2TP status - authentication states

The states associated with the LNS or LAC authentication are:

Value	Description
noAuthentication	Authentication is not enabled. This is also the start-up state for the authentication process.
authenSuccessful	Authentication was successful. The Telindus 1031 Router remains in this state during data transfer.
authenFailure	Authentication failed. This is a transient state since the Telindus 1031 Router starts the handshake again after a failing authentication.

11.6 Bridge status attributes

telindus1031/bridge/bridgeGroup/ifDescr

This attribute displays the interface description. This is an SNMP MIB2 parameter.

telindus1031/bridge/bridgeGroup/ifType

This attribute displays the interface type. This is an SNMP MIB2 parameter.

telindus1031/bridge/bridgeGroup/ifOperStatus

This attribute displays the current operational status of the bridge group. This is an SNMP MIB2 parameter.

telindus1031/bridge/bridgeGroup/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface. This is an SNMP MIB2 parameter.

telindus1031/bridge/bridgeGroup/ip

This attribute displays the IP information of the bridge.

The ip structure contains the following elements:

Element	Description
address	This is the IP address of the bridge. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the interface. It is either configured or retrieved automatically.

telindus1031/bridge/bridgeGroup/arpCache

This attribute displays all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface. Refer to What is the ARP cache? on page 179 for more information.

The arpCache table contains the following elements:

Element	Description
macAddress	This is the MAC address.
ipAddress	This is the associated IP address.
type	This is the ARP cache entry type. Possible values are: **Value** / **Description** dynamic: The MAC - IP address pair is retrieved from an ARP request or reply message. static: The MAC - IP address pair is configured. There is only one static entry, i.e. the Telindus 1031 Router its own IP and MAC address.
timeOut	This is the time the entry will remain in the ARP cache. For the static entry, this value is 0.

telindus1031/bridge/bridgeGroup/bridgeCache

When a port of the bridge enters the learning state, it stores the MAC addresses of the stations situated on the network that is connected to this port. The MAC addresses are stored in a MAC address database or bridge cache. The bridgeCache attribute visualises this address database. Refer to What is the bridge cache? on page 232 for more information.

The bridgeCache table contains the following elements:

Element	Description
interface	This is the interface through which the station can be reached.
macAddress	This is the MAC address of the station situated on the network connected to the interface.
type	This displays whether the MAC address entry is static or dynamic: **Value** / **Description** dynamic: The corresponding MAC address is learned on one of the interfaces. static: There are only two static entries: • the Telindus 1031 Router its own MAC address • a MAC address used for Spanning Tree.
age	This is the elapsed time since a frame was received from the station.

Example

The following figure shows part of a bridge cache table as an example:

bridgeCache

	interface	macAddress	type	age
1	Bridge Protocol Entity	01:80:c2:00:00:00	static	00000d 00h 00m 00s
2	Bridge Protocol Entity	00:c0:89:00:fe:20	static	00000d 00h 00m 00s
3	lan	00:c0:89:00:d4:56	dynamic	00000d 00h 00m 01s
4	lan	00:c0:89:00:70:98	dynamic	00000d 00h 00m 09s
5	lan	00:c0:89:00:6b:9c	dynamic	00000d 00h 00m 16s
6	lan	00:c0:89:01:26:86	dynamic	00000d 00h 00m 05s
7	lan	00:10:b5:ec:3f:24	dynamic	00000d 00h 00m 00s
8	lan	00:a0:24:a2:97:6c	dynamic	00000d 00h 01m 25s
9	lan	00:c0:89:00:d4:53	dynamic	00000d 00h 01m 53s
10	lan	00:60:8c:95:bb:fe	dynamic	00000d 00h 00m 00s
11	lan	00:10:4b:47:38:fa	dynamic	00000d 00h 00m 15s
12	lan	00:c0:89:00:d4:c2	dynamic	00000d 00h 01m 40s

telindus1031/bridge/bridgeGroup/bridging

The bridging attributes or elements in the individual interface objects display the bridging information for that particular interface. This bridging attribute, however, displays the bridging information of all the (bridged) interfaces of the Telindus 1031 Router.

Refer to telindus1031/lanInterface/bridging on page 254 for a detailed description of the bridging structure. Note however that the bridge group bridging structure contains one extra element: name. This is the name of the interface as you configured it. Note that the interface can also be a DLCI, an ATM PVC, a tunnel, etc.

telindus1031/bridge/bridgeGroup/spanningTree

This attribute gives you the Spanning Tree status information of the bridge.

The spanningTree structure contains the following elements:

Element	Description
designatedPriority	Together, these two elements form the unique bridge identifier.
designatedMAC	They display the unique bridge identifier of the root bridge as it is indicated in the root identifier parameter of the Configuration BPDUs. These BPDUs are transmitted by the designated bridge for the LAN that is currently connected to this port. This bridge identifier is used to test the value of the root identifier parameter conveyed in received Configuration BPDUs.
rootPathCost	This is the cost of the path from this bridge to the root bridge. If this bridge is the root bridge, the rootPathCost value equals 0. Else, the rootPathCost value equals the sum of … • the path cost as it is up to the designated bridge for the LAN that is currently connected to this port (this cost is transmitted in Configuration BPDUs by the designated bridge) and • the path cost as it is configured for the root port. The rootPathCost element is used … • to test the value of the root path cost parameter conveyed in received Configuration BPDUs. • as the value of the root path cost parameter in transmitted Configuration BPDUs. The total cost of the path to the root bridge should not exceed 65500.
rootPort	This is the port identifier of the port that offers the lowest cost path to the root. If two or more ports offer equal least cost paths to the root bridge, then the root port is selected to be that with the highest designatedPriority (i.e. the lowest numerical value). If two or more ports offer equal least cost paths to the root bridge and the same designatedPriority, then the root port is selected to be that with the highest designatedPortPriority (i.e. the lowest numerical value).

Element	Description
bridgePriority	Together, these two attributes form the unique bridge identifier of this bridge.
bridgeMAC	
maxAge	This is the time-out value to be used by all bridges in the bridged LAN for discarding bridging information. The maxAge element displays the value as it is set by the root bridge. This information is conveyed by the root bridge to ensure that each bridge in the bridged LAN has a consistent value against which to test the age of stored configuration information.
helloTime	This is the interval between the generation of Configuration BPDUs by the root bridge. The helloTime element displays the value as it is set by the root bridge. This attribute is not directly used by the Spanning Tree algorithm, but it is conveyed by the root bridge to facilitate the monitoring of protocol performance by the management system.
forwardDelay	This is the time-out value to be used by all bridges in the bridged LAN for … • a bridge port applies to move from listening state to learning state or from learning state to forwarding state. • time-out (or ageing) for purging MAC addresses from the bridge cache in case a topology change is detected. The forwardDelay element displays the value as it is set by the root bridge. This information is conveyed by the root bridge to ensure that each bridge in the bridged LAN has a consistent value for the forward delay timer.
topologyChange	This is a Boolean value (0 or 1) to report … • for a bridge that is not a root bridge, whether or not the most recently accepted Configuration BPDU indicates a change in the active topology. • for the root bridge, whether or not a change in topology has been detected within the preceding topologyChangeTime period. The topologyChange element is used to … • propagate the topology change indication in transmitted Configuration BPDUs. • determine whether the short (bridgeForwardDelay) or long (bridgeTimeOut) time-out (or ageing) value is used to purge dynamic MAC addresses from the bridge cache.
topologyChange-Detection	This is a Boolean value (0 or 1) to report that a topology change has been detected by or notified to the bridge.
topologyChange-Time	This displays the time during which the root bridge transmits Configuration BPDUs indicating a topology change, after it detected this topology change. The topologyChangeTime element value is equal to the sum of the root bridge its bridgeMaxAge element value and bridgeForwardDelay element value. Refer to telindus1031/bridge/bridgeGroup/spanningTree on page 234 for more information on the latter two elements.

telindus1031/bridge/bridgeGroup/clearArpCache

If you execute this action, the ARP cache table is cleared.

telindus1031/bridge/bridgeGroup/clearBridgeCache

If you execute this action, the bridge cache table is cleared.

11.7 Management status attributes

telindus1031/management/cms2Address

This attribute displays the absolute device address as you configured it.

Loop-back status attributes

telindus1031/management/loopback/ifDescr

This attribute displays the interface description. This is an SNMP MIB2 parameter.

telindus1031/management/loopback/ifType

This attribute displays the interface type. This is an SNMP MIB2 parameter.

telindus1031/management/loopback/ifOperStatus

This attribute displays the current operational status of the loop-back interface. This is an SNMP MIB2 parameter.

The loop-back interface is always up.

telindus1031/management/loopback/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface. This is an SNMP MIB2 parameter.

telindus1031/management/loopback/ipAddress

This attribute displays the IP address of the loop-back interface as you configured it.

11.8 File system status attributes

telindus1031/fileSystem/fileList

Part of the flash memory of the Telindus 1031 Router is organised as a file system and a number of files are stored in it. The fileList attribute shows all the files that are present on the file system. Usually, the following files are present:

- The configuration file of the Telindus 1031 Router (file config1.db).
- Up to two application software files of the Telindus 1031 Router (files CONTROL1 and CONTROL 2).

The fileList table contains the following elements:

Element	Description
name	This is the file name. Maximum length of the file name is 24 characters. All characters are allowed (including spaces). The file name is case sensitive.
length	This is the length of the file in bytes.

telindus1031/fileSystem/freeSpace

This attribute displays the number of free bytes on the file system.

telindus1031/fileSystem/status

This attribute displays the status of the file system. Possible values are:

Value	Description
ready	Normal situation.
formatting	The file system is being formatted. This can be triggered when the file system is found to be corrupt at boot.
corrupt	The file system is in a state were no guarantee can be given about the correct operation of the file system. The file system will be formatted at the following boot.
corruptBlocks	A certain block can not be erased.

telindus1031/fileSystem/corruptBlocks

The file system of the Telindus 1031 Router consists of several blocks. When a block can not be erased, the corruptBlocks count is incremented. This block can no longer be used to store data.

telindus1031/fileSystem/Delete File

Use this action to remove obsolete files from the file system. You have to enter the file name you want to delete as argument value.

telindus1031/fileSystem/Rename File

Use this action to rename a file on the file system. You have to enter the old and new file name in a structure.

File names are case sensitive.

11.9 Operating system status attributes

telindus1031/operatingSystem/taskInfo

This attribute displays status information about the operating system.

The taskInfo table contains the following elements:

Element	Description
taskName	This is the name of the task.
taskStatus	This is the current status of the task. Possible values are: **Value** / **Description** awake — This task is actually running. asleep — This task is waiting on an event. inactive — This task slot is not active, i.e. no task has been assigned to this slot.
load30s	This is the load on the processor, in percent, during the last 30 seconds.
load5m	This is the load on the processor, in percent, during the last 5 minutes.
runningInMedium	Each task can be running with a low, medium or high priority. This element gives the percentage of time this task has been running with medium priority during the last 30 seconds.
runningInHigh	Each task can be running with a low, medium or high priority. This element gives the percentage of time this task has been running with high priority during the last 30 seconds. The percentage of time this task has been running with low priority can be calculated using the following formula: running in low priority = 100% - runningInMedium - runningInHigh
programCounter	This is the current value of the program counter. The program counter is the memory address for the current instruction of this task.

11.10 Proxy status attributes

Refer to the Telindus 1030 Router Orchid function manual for more information on the status attributes of the proxy function (also called Orchid function).

12 Performance attributes

This chapter discusses the performance attributes of the Telindus 1031 Router. The following gives an overview of this chapter:

- 12.1 - Performance attributes overview on page 300
- 12.2 - LAN interface performance attributes on page 302
- 12.3 - WAN interface performance attributes on page 305
- 12.4 - Router performance attributes on page 312
- 12.5 - Bridge performance attributes on page 318
- 12.6 - Management performance attributes on page 321
- 12.7 - Operating system performance attributes on page 323
- 12.8 - Proxy performance attributes on page 325

12.1 Performance attributes overview

> telindus1031

>> lanInterface
- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- h2Performance
- h24Performance

>> g703[1]
- errorCount

>>> channel[g703_1]
- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- ifOutPQLen
- h2Performance
- h24Performance

>>>> frameRelay
- dlciTable
- lmi
- cllmInFrames

>>>> atm
- pvcTable
- unknownCells

>> router
- routingTable
- pingResults
- Action: startPing
- Action: stopPing

>>> defaultNat
- socketsFree
- allocFails
- discards
- addressesAvailable
- tcpSocketsUsed
- udpSocketsUsed
- icmpSocketsUsed
- tcpAllocs
- udpAllocs
- icmpAllocs
- Action: resetNat

>>> tunnels
- l2tpTunnels

>> bridge

>>> bridgeGroup
- bridgeCache
- bridgeDiscards
- bridgeFloods

>>> accessList[ ]
- bridgeAccessList

>> management
- cms2SessionCount
- tftpSessionCount
- cliSessionCount
- tcpSessionCount

>> operatingSystem

currUsedProcPower
usedProcPower
freeDataBuffers
totalDataBuffers
largestFreeBlockSize
freeBlockCount
freeMemory
totalMemory
taskInfo

>> proxy

Refer to the Telindus 1030 Router Orchid function manual for more information on the performance attributes of the proxy function (also called Orchid function).

12.2 LAN interface performance attributes

telindus1031/lanInterface/ifInOctets

This attribute displays the number of octets (bytes) received on this interface.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifInUcastPkts

This attribute displays the number of unicast packets received on this interface and delivered to a higher-layer protocol. Unicast packets are all non-multicast and non-broadcast packets.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifInNUcastPkts

This attribute displays the number of non-unicast packets received on this interface and delivered to a higher-layer protocol. Non-unicast packets are all the multicast and broadcast packets.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifInDiscards

This attribute displays the number of incoming packets that were discarded, to prevent their deliverance to a higher-layer protocol. This even though no errors were detected in these packets.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifInErrors

This attribute displays the number of incoming packets that could not be delivered to a higher-layer protocol because they contained errors.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifInUnknownProtos

This attribute displays the number of incoming packets that were discarded because they contained an unknown or unsupported protocol.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOutOctets

This attribute displays the total number of octets (bytes) transmitted by the interface, including framing characters.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOutUcastPkts

This attribute displays the total number of packets that higher-level protocols requested to be transmitted to a unicast address, including those that were discarded or not sent.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOutNUcastPkts

This attribute displays the number of non-unicast packets that higher-level protocols requested to be transmitted to a non-unicast (i.e. a broadcast or multicast) address, including those that were discarded or not sent.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOutDiscards

This attribute displays the number of outgoing packets that were discarded, to prevent they are transmitted by the interface. This could be due to, for instance, the presence of an access list.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOutErrors

This attribute displays the number of outgoing packets that could not be transmitted by the interface because they contained errors.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/ifOutQLen

This attribute displays the length, expressed in packets, of the output packet queue on the interface.

This is an SNMP MIB2 parameter.

telindus1031/lanInterface/h2Performance

This attribute displays the 2 hours performance summary of the LAN interface.

The h2Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
ifUpTime	the time during which the interface was up.
ifStatusChanges	the number of times the ifOperStatus value of the interface changed (from up to down or vice versa).
ifInOctets	the number of octets (bytes) received on this interface.
ifInPackets	the number of packets received on this interface.
ifInErrors	the number of packets received on this interface that could not be delivered to a higher-layer protocol because they contained errors.
ifOutOctets	the number of octets (bytes) transmitted by the interface, including framing characters.
ifOutPackets	the number of packets transmitted by the interface.
ifOutDiscards	the number of outgoing packets that were discarded, to prevent they were transmitted by the interface. This could be due to, for instance, the presence of an access list.
ifOutErrors	the number of packets that could not be transmitted by the interface because they contained errors.

telindus1031/lanInterface/h24Performance

This attribute displays the 24 hours performance summary of the LAN interface. The h24Performance table contains the same elements as the telindus1031/lanInterface/h2Performance table.

12.3 WAN interface performance attributes

This section discusses the performance attributes of the WAN interface. First it describes the performance attributes of the physical interface. Then it explains the performance attributes of the encapsulation protocols that can be used on the interface.

The following gives an overview of this section:

- 12.3.1 - G703 interface performance attributes on page 306
- 12.3.2 - G703 channel performance attributes on page 307
- 12.3.3 - Frame Relay performance attributes on page 308
- 12.3.4 - ATM performance attributes on page 311

12.3.1 G703 interface performance attributes

telindus1031/g703[ ]/errorCount

In case CRC4 insertion is enabled, this attribute displays the amount of CRC4 errors that were detected on the interface. Refer to telindus1031/g703[ ]/crc4Insertion on page 183 for more information on CRC4 insertion.

12.3.2 G703 channel performance attributes

Most performance attributes of the WAN interface are the same as on the LAN interface. Therefore, they are not explained here again. Refer to 12.2 - LAN interface performance attributes on page 302 for a complete description of these attributes.

However, the attribute ifOutPQLen is only present on the WAN interface and therefore explained below.

telindus1031/g703[ ]/channel[ ]/ifOutPQLen

In case an overload condition occurs and priority queuing is activated, then this attribute displays how many packets the different queues contain.

This is an SNMP MIB2 parameter.

12.3.3 Frame Relay performance attributes

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable

This attribute lists the complete performance information of all known DLCIs.

The dlciTable table contains the following elements:

Element	Description
name	This is the name of the DLCI as you configured it.
mibCounters	This displays the SNMP MIB2 parameters of the DLCI. These are the same as the SNMP MIB2 parameters on the LAN interface. Refer to 12.2 - LAN interface performance attributes on page 302.
frameRelay	This displays the specific Frame Relay related performance information of the DLCI. Refer to telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay on page 309 for a detailed description of the frameRelay structure.

telindus1031/g703[ ]/channel[ ]/frameRelay/dlciTable/frameRelay

The frameRelay structure in the dlciTable displays the specific Frame Relay related performance information of the DLCI.

The frameRelay structure contains the following elements:

Element	Description
dlci	This is the DLCI identification number.
inFecn	This is the number of frames received from the network indicating forward congestion and this since the virtual circuit was created.
inBecn	This is the number of frames received from the network indicating backward congestion and this since the virtual circuit was created.
inDe	This is the number of frames received with the Discard Eligibility bit set.
inOctets	This is the number of octets received over this virtual circuit since it was created.
inFrames	This is the number of frames received over this virtual circuit since it was created.
outFecn	This is the number of frames sent to the network indicating forward congestion and this since the virtual circuit was created.
outBecn	This is the number of frames sent to the network indicating backward congestion and this since the virtual circuit was created.
outDe	This is the number of frames sent to the network with the Discard Eligibility bit set.
outOctets	This is the number of octets sent over this virtual circuit since it was created.
outFrames	This is the number of frames sent over this virtual circuit since it was created.

telindus1031/g703[ ]/channel[ ]/frameRelay/lmi

This attribute gives a complete LMI performance overview.

The lmi structure contains the following elements:

Element	Description
inStatusEnquiry	This is the number of Status Enquiries received from the network.
inStatus	This is the number of Status Reports received from the network.
inStatusUpdate	This is the number of unsolicited Status Updates received from the network.
outStatusEnquiry	This is the number of Status Enquiries sent to the network.
outStatus	This is the number of Status Reports sent to the network.
outStatusUpdate	This is the number of unsolicited Status Updates sent to the network.
netPollNotRcvd	This is the number of times the expectedPollInterval expired without an incoming status enquiry.
userNoResponse-Rcvd	This is the number of times a response was not received.
userBadResponses-Rcvd	This is the number of times an invalid response was received.

telindus1031/g703[ ]/channel[ ]/frameRelay/cllmInFrames

This attribute displays the total number of received CLLM (Consolidated Link Layer Management) frames.

12.3.4 ATM performance attributes

telindus1031/g703[ ]/channel[ ]/atm/pvcTable

This attribute lists the complete performance information of all known PVCs.

The pvcTable table contains the following elements:

Element	Description
name	This is the name of the PVC as you configured it.
mibCounters	This displays the SNMP MIB2 parameters of the PVC. These are the same as the SNMP MIB2 parameters on the LAN interface. Refer to 12.2 - LAN interface performance attributes on page 302.
priorityQLengths	In case an overload condition occurs and priority queuing is activated, then this elements displays how many packets the different queues contain.
atm	This displays the specific ATM related performance information of the PVC. The atm structure contains the following elements:

Element	Description
vpi	This displays the Virtual Path Identifier (VPI) of the PVC.
vci	This displays the Virtual Channel Identifier (VCI) of the PVC. The VPI in conjunction with the VCI identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.

telindus1031/g703[ ]/channel[ ]/atm/unknownCells

This attribute displays the number of received cells that are not treated by the Telindus 1031 Router. For example, data cells for PVCs that are not configured in the Telindus 1031 Router, etc.

12.4 Router performance attributes

This section discusses the performance attributes concerned with routing. First it describes the general routing performance attributes. Then it explains the performance attributes of the extra features as there are default NAT, filtering, L2TP tunnelling, etc…

The following gives an overview of this section:

- 12.4.1 - General router performance attributes on page 313
- 12.4.2 - Default NAT performance attributes on page 315
- 12.4.3 - L2TP tunnel performance attributes on page 317

12.4.1 General router performance attributes

telindus1031/router/routingTable

This attribute lists all known routes and how many times they are used.

The routingTable contains the following elements:

Element	Description
network	This is the IP address of the destination network.
mask	This is the network mask of the destination network.
gateway	This is the IP address of the next router on the path to the destination network.
interface	This is the interface through which the destination network can be reached. Possible values are: **Value** / **Description** internal: The own protocol stack is used. <name>: The destination network can be reached through this particular interface. The <name> of the interface is the name as you configured it. Note that the “interface” can also be a DLCI, an ATM PVC, a tunnel, etc. discard: Packets for this destination are discarded.
uses	This lists how many times the route has been used since it is listed in the routing table. For each IP packet that matches this route, the attribute value is incremented by one. RIP routes may disappear from the routing table, and re-appear afterwards. The attribute value is reset when a RIP route disappears from the routing table.

telindus1031/router/pingResults

Use this action to send a ping to an IP address (only one ping at a time). You can start and stop pinging with the ping actions startPing and stopPing. The pingResults attribute lists the results of the transmitted ping.

The routingTable contains the following elements:

Element	Description
ipAddress	This is the IP address being pinged.
numOfTxPackets	This is the number of transmitted pings.
numOfRxPackets	This is the number of correct received answers on the transmitted pings.
minReplyTime	This is the lowest reply time of all correct received answers.
maxReplyTime	This is the highest reply time of all correct received answers.
avrgReplyTime	This is the average reply time of all correct received answers.

telindus1031/router/startPing

Execute this actions to start transmitting pings to an IP address. Several arguments can be set:

Argument	Description
ipAddress	This is the IP address you want to ping. Default:0.0.0.0 Range: up to 255.255.255.255
iterations	This is the number of pings. If you enter 0, the IP address will be pinged an indefinite number of times. The only way to stop the ping session is by executing the stopPing action. Default:5 Range: 0 …
interval	This is the interval, in seconds, between consecutive pings. Default:1 Range: 0 … 100
dataLength	This is the length of the data transmitted in a ping. Default:31 Range: 0 … 1300
timeOut	If a ping is sent, the system will wait for a certain period on the answer. I.e. the system expects the answer within this period. Use the timeOut argument to set this period. Default:00000d 00h 00m 05s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

telindus1031/router/stopPing

Stops the pending pings.

12.4.2 Default NAT performance attributes

telindus1031/router/defaultNat/socketsFree

This attribute shows the remaining number of new connections (i.e. sockets) that can be initiated. A socket is a set of source and destination IP addresses and port numbers.

Initially, 2048 simultaneous sockets can be initiated. Sockets are freed using a garbage mechanism. This means that every five minutes all sockets are checked. If a socket has been released by PAT or NAT, then this socket is returned to the pool of free sockets.

ICMP and UDP sockets are released when they have no data traffic during five minutes. TCP sockets are released after the TCP session has been closed or when the session has been idle for 24 hours.

telindus1031/router/defaultNat/allocFails

If no sockets are available anymore but an attempt to set up a new connection is being made, then the natAllocFails attribute value is incremented by 1.

Because the sockets are distributed using a hashing function, it is possible that natAllocFails increases even though natSocketsFree still indicates free sockets.

ICMP requires a new socket for each transmitted packet. This implies that, for instance, a permanent ping or trace-route command may eventually use all free sockets.

telindus1031/router/defaultNat/discards

This attribute indicates how many times a packet has been discarded for reasons other than a lack of free sockets. This could be, for instance, because an attempt was made to connect from the Internet to a service that was not present in the servicesAvailable table.

telindus1031/router/defaultNat/addressesAvailable

This attribute displays the number of NAT addresses that are currently free.

telindus1031/router/defaultNat/tcpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for TCP applications.

telindus1031/router/defaultNat/udpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for UDP applications.

telindus1031/router/defaultNat/icmpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for ICMP applications.

telindus1031/router/defaultNat/tcpAllocs

This attribute indicates how many TCP sockets have been allocated since cold boot. Together with the performance attributes natUdpAllocs and natIcmpAllocs it gives an indication of the type of traffic that is being routed.

telindus1031/router/defaultNat/udpAllocs

This attribute indicates how many UDP sockets have been allocated since cold boot. Together with the performance attributes natTcpAllocs and natIcmpAllocs it gives an indication of the type of traffic that is being routed.

telindus1031/router/defaultNat/icmpAllocs

This attribute indicates how many ICMP sockets have been allocated since cold boot. Together with the performance attributes natTcpAllocs and natUdpAllocs it gives an indication of the type of traffic that is being routed.

telindus1031/router/defaultNat/resetNat

Use this action to release all sockets currently in use and return them to the free socket pool.

In other words, executing this action resets all NAT/PAT sessions that are currently established. It also releases all official IP addresses that are dynamically assigned to a private IP address. If any TCP sessions are still active, these sessions will be aborted.

Take care when using this action! All TCP information is lost when the sockets are released with this action. Any TCP sessions in use at the time of the reset will go into a hang-up state. These applications will need to restart.

12.4.3 L2TP tunnel performance attributes

telindus1031/router/tunnels/l2tpTunnels

This attribute gives you performance information on the L2TP tunnels.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel as you configured it.
mibCounters	This displays the SNMP MIB2 parameters of the tunnel. These are the same as the SNMP MIB2 parameters on the LAN interface. Refer to 12.2 - LAN interface performance attributes on page 302.

12.5 Bridge performance attributes

This section discusses the performance attributes concerned with bridging. First it describes the general bridging performance attributes. Then it explains the performance attributes of the extra features as there are access listing, etc…

The following gives an overview of this section:

- 12.5.1 - Bridge group performance attributes on page 319
- 12.5.2 - Bridge access list performance attributes on page 320

12.5.1 Bridge group performance attributes

telindus1031/bridge/bridgeGroup/bridgeCache

When a port of the bridge enters the learning state, it stores the MAC addresses of the stations situated on the network that is connected to this port. The MAC addresses are stored in a MAC address database or bridge cache. The bridgeCache attribute visualises this address database. Refer to What is the bridge cache? on page 232 for more information.

The bridgeCache table contains the following elements:

Element	Description
interface	This is the interface through which the station can be reached.
macAddress	This is the MAC address of the station situated on the network connected to the interface.
rxCount	This is the number of frames received from the corresponding MAC address.
txCount	This is the number of frames forwarded to the corresponding MAC address.

telindus1031/bridge/bridgeGroup/bridgeDiscards

This attribute displays the number of times a frame was discarded because …

- it was received on the same interface as the one through which the destination address can be reached.
- it was received on an interface that is not in the forwarding state.

telindus1031/bridge/bridgeGroup/bridgeFloods

This attribute displays the number of times a frame was flooded on all interfaces because …

- it was a broadcast / multicast.
- the position of the station with the destination MAC address was not known (yet).

12.5.2 Bridge access list performance attributes

telindus1031/bridge/accessList[ ]/bridgeAccessList

This attribute shows information on the use of the bridge access list.

The bridgeAccessList table contains the following elements:

Element	Description
macAddress	This is the MAC address as configured in the configuration attribute telindus1031/bridge/accessList[ ]/bridgeAccessList.
uses	This indicates the number of times a packet has been discarded for the corresponding MAC address.

12.6 Management performance attributes

telindus1031/management/cms2SessionCount

This attribute displays the number of CMS2 sessions that are currently active on the Telindus 1031 Router.

There are always minimum two fixed sessions active. Connecting with TMA, TMA CLI, Telnet, etc. opens additional sessions. This is explained in the following table:

Session count	Purpose
1 fixed session	A fixed session for SNMP.
1 fixed session	A fixed session for O10.
+ 2 sessions	When connecting with TMA.
+ 1 session	When connecting with TMA for HP OpenView or the Alarm Manager.
+ 1 session	When connecting with TMA CLI.
+ 2 sessions	When downloading a config.cli or config.cms file.
+ 1 session	When connecting with Telnet.
+ 1 session	When downloading software.
+ 1 session	When connecting with the Web Interface.

telindus1031/management/tftpSessionCount

This attribute displays the number of TFTP sessions that are currently active on the Telindus 1031 Router.

telindus1031/management/cliSessionCount

This attribute displays the number of CLI sessions that are currently active on the Telindus 1031 Router.

There are always minimum two fixed sessions active. Connecting with TMA CLI, the Web Interface, etc. opens additional sessions. This is explained in the following table:

Session count	Purpose
1 fixed session	A fixed session for the control port.
1 fixed session	A fixed session for Web Interface.
+ 1 session	When connecting with TMA CLI or starting a CLI session.
+ 1 session	When connecting with the Web Interface.

telindus1031/management/tcpSessionCount

This attribute displays the number of TCP sessions that are currently active on the Telindus 1031 Router. The following table shows when a TCP session opens:

Session count	Purpose
+ 1 session	When connecting with Telnet.
+ 1 session	When connecting with the Web Interface.

12.7 Operating system performance attributes

telindus1031/operatingSystem/currUsedProcPower

This attribute displays the amount of processing power used during the last 650 milliseconds, expressed as a percentage of the total available processing power.

telindus1031/operatingSystem/usedProcPower

This attribute lists the used processing power for the 11 most recent 30 seconds intervals. The processing power is expressed as a percentage of the total processing power.

The usedProcPower table contains the following elements:

Element	Description
sysUpTime	This is the elapsed time since the last cold boot. The next values are for the 30 seconds period before this relative time stamp.
min	This is the minimum percentage of processing power in use during the last 30 seconds.
average	This is the average percentage of processing power in use during the last 30 seconds.
max	This is the maximum percentage of processing power in use during the last 30 seconds.

telindus1031/operatingSystem/freeDataBuffers

The processor uses buffers for storing the packets during processing and/or queuing. Each buffer has a 256 byte size, headers included. This attribute is the number of data buffers currently not in use and available for e.g. incoming data.

telindus1031/operatingSystem/totalDataBuffers

This attribute displays the total number of available data buffers.

telindus1031/operatingSystem/largestFreeBlockSize

The processor uses RAM memory for storing internal information and buffering. The different tasks allocate RAM memory on request. Tasks may also free memory again. In this way the total RAM memory becomes fragmented. This attribute gives the size of the largest contiguous free memory block expressed in bytes.

telindus1031/operatingSystem/freeBlockCount

This attribute displays the number of free contiguous memory blocks.

telindus1031/operatingSystem/freeMemory

This attribute displays the total free memory expressed in bytes.

telindus1031/operatingSystem/totalMemory

This attribute displays the total RAM memory expressed in bytes.

telindus1031/operatingSystem/taskInfo

This attribute contains status information concerning the different tasks running on the processor. It is a table grouping up to 31 task slots, which is the maximum number of parallel tasks running on the processor's operating system.

This attribute contains the same elements as the status attribute telindus1031/operatingSystem/taskInfo on page 296.

12.8 Proxy performance attributes

Refer to the Telindus 1030 Router Orchid function manual for more information on the performance attributes of the proxy function (also called Orchid function).

13 Alarm attributes

This chapter discusses the alarm attributes of the Telindus 1031 Router. The following gives an overview of this chapter:

- 13.1 - Alarm attributes overview on page 328
- 13.2 - Introducing the alarm attributes on page 329
- 13.3 - General alarms on page 332
- 13.4 - LAN interface alarms on page 334
- 13.5 - G703 interface alarms on page 335
- 13.6 - G703 channel alarms on page 336
- 13.7 - Router alarms on page 337

13.1 Alarm attributes overview

> telindus1031
totalAlarmLevel
alarmInfo
notResponding
alarmSyncLoss
configChanged
access
unknownStatus
coldBoot
warmBoot
codeConsistencyFail
configConsistencyFail

>> lanInterface
alarmInfo
linkDown

>> g703[1]
alarmInfo
linkDown
lfa
ais
sevErroredSec

>>> channel[g703_1]
alarmInfo
linkDown

>> router
alarmInfo
pingActive

13.2 Introducing the alarm attributes

Before discussing the alarm attributes of the Telindus 1031 Router in detail, some general information on the alarm attributes of the Telindus 1031 Router is given.

The following gives an overview of this chapter:

- 13.2.1 - Configuration alarm attributes on page 330
- 13.2.2 - General alarm attributes on page 331

13.2.1 Configuration alarm attributes

telindus1031/.../alarmMask

Use this attribute to enable (unmasked) or disable (masked) for each alarm of the corresponding object, whether it is communicated to the central management system (e.g. HP OpenView) or not.

Alarms are always seen in the alarmInfo alarm attribute of an object, regardless of the masking of the alarm. I.e. even if an alarm is set to disabled in the alarmMask of an object, if the alarm condition is fulfilled then the alarm will be set to on in the alarmInfo of that object. However, because this alarm is disabled it will not be sent to the central management system (e.g. HP OpenView).

Only the most important alarms are unmasked (i.e. enabled) by default. All other alarms are masked (i.e. disabled).

telindus1031/.../alarmLevel

Use this attribute to assign a priority level to each alarm of the corresponding object. The alarm level range goes from 0 to 254, where 0 is the lowest and 254 is the highest priority level.

The alarmLevel of an unmasked, active alarm is sent to the totalAlarmLevel alarm attribute of the top object telindus1031.

13.2.2 General alarm attributes

telindus1031/totalAlarmLevel

This attribute is only present in the top object of the containment tree of the Telindus 1031 Router, being telindus1031.

It displays the priority level of an unmasked, active alarm. When several alarms are generated at the same time, the highest priority level is shown. If the alarm levels are set in a structured manner, one look at the totalAlarmLevel attribute enables the operator to make a quick estimation of the problem.

The value of the totalAlarmLevel attribute is also communicated to the central management system (e.g. HP OpenView) where it determines the colour of the icon. This colour is an indication of the severity of the alarm.

telindus1031/…/alarmInfo

This attribute contains the actual alarm information of the corresponding object.

The alarmInfo structure contains the following elements:

Element	This element displays for the corresponding object …
discriminator	the total alarm count since the last cold boot.
currentAlarms	the current alarms.
previousAlarms	the second most recent alarms.
alarmMask	the alarmMask as you configured it.
alarmLevel	the alarmLevel as you configured it.

13.3 General alarms

Refer to 13.2 - Introducing the alarm attributes on page 329 for general information on the alarm attributes.

telindus1031/alarmInfo

The different alarms related to the telindus1031 object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
notResponding	by the management concentrator when the Telindus 1031 Router does not respond on its polling session.	enabled	4
alarmSyncLoss	when the internal alarm buffer overflows.	enabled	4
configChanged	when the local configuration has been changed.	disabled	1
access	when a management session is started on the Telindus 1031 Router itself. This alarm is not activated when the management session is established through a management concentrator. **Example** The alarm is *activated* in case of … • a TMA, TMA CLI, terminal (CLI or ATWIN) or EasyConnect session via the control connector of the Telindus 1031 Router. • a TMA, TMA CLI, TMA for HP OpenView, Telnet (CLI or ATWIN), HTTP (Web Interface) or TFTP session using the LAN / WAN IP address of the Telindus 1031 Router. The alarm is *not activated* in case of … • any management session (TMA, terminal, Telnet, HTTP, etc.) established *through a management concentrator* on the Telindus 1031 Router. • SNMP management.	disabled	1
unknownState	each time a new Telindus 1031 Router is added to the network and before the management concentrator has completed a first successful polling session.	disabled	0
coldBoot	each time the Telindus 1031 Router performs a cold boot.	disabled	1

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
warmBoot	each time the Telindus 1031 Router performs a warm boot.	disabled	1
codeConsistency-Fail	when the software consistency imposed by the management concentrator on the Telindus 1031 Router fails. For example, because of a loss of contact. Check the status attribute o1003/nmsgroup/softConsistencyStatus to determine the problem.	disabled	1
configConsistency-Fail	when the configuration consistency imposed by the management concentrator on the Telindus 1031 Router fails. For example, because of a loss of contact. Check the status attributes o1003/nmsgroup/objectTable/configState and configDiag to determine the problem.	disabled	1

13.4 LAN interface alarms

Refer to 13.2 - Introducing the alarm attributes on page 329 for general information on the alarm attributes.

telindus1031/lanInterface/alarmInfo

The alarm related to the lanInterface object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when no valid LAN data is detected. I.e. when the connection between the interface and the LAN is down.	enabled	3

13.5 G703 interface alarms

Refer to 13.2 - Introducing the alarm attributes on page 329 for general information on the alarm attributes.

telindus1031/g703[ ]/alarmInfo

The alarms related to the g703[ ] object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when the incoming data is no longer present. E.g. the connection *from* the WAN *towards* the Telindus 1031 Router is interrupted.	disabled	3
lfa	when the Frame Alignment Signal (FAS), which is present in time slot 0 of the G.704 framed data, is not detected after a certain period. This alarm is also generated when the crc4Insertion attribute is set to enabled, but no CRC is present in the incoming data. (This does not apply when crc4Insertion is set to auto.)	disabled	2
ais	when the AIS signal (also called *all ones*) is detected on the incoming data. E.g. a device / application in the network detected a problem and communicates this to the other devices in the network.	disabled	2
sevErroredSec	when a severely erroneous second is detected.	disabled	2

13.6 G703 channel alarms

Refer to 13.2 - Introducing the alarm attributes on page 329 for general information on the alarm attributes.

telindus1031/g703[ ]/channel[ ]/alarmInfo

The alarm related to the g703[ ]/channel[ ] object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when an error situation is detected in the encapsulation protocol (Frame Relay, PPP or ATM). For instance, an error condition in the Frame Relay LMI, a failed authentication in PPP, …	enabled	3

13.7 Router alarms

Refer to 13.2 - Introducing the alarm attributes on page 329 for general information on the alarm attributes.

telindus1031/router/alarmInfo

The alarm related to the router object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
pingActive	in case of a pending ping (for example, an indefinite ping). This notification is necessary because you can only transmit one ping at a time. Furthermore, there is no protection when a new ping is started before the previous is stopped.	enabled	3

14 TMA sub-system picture

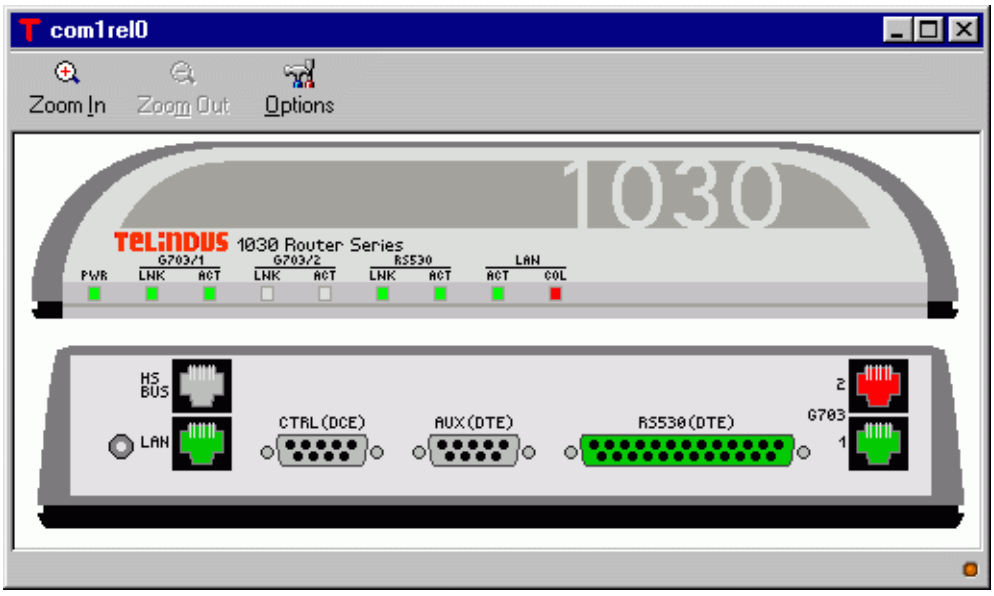
The sub-system picture is a TMA tool that visualises the status information of the Telindus 1031 Router. This chapter explains how to display the sub-system picture, and how to interpret the visual indications.

How to display the sub-system picture?

To display the sub-system picture of the Telindus 1031 Router, click on the sub-system picture button located in the TMA toolbar: .

Structure of the sub-system picture

This paragraph displays and labels the different elements of the sub-system picture. It also explains how the visual indications should be interpreted. Below, the Telindus 1031 Router sub-system picture is displayed:



The following table gives an overview of the sub-system picture elements and what they indicate:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>LEDs</td><td>These reflect the actual status of the device.

The LED indication on the sub-system picture corresponds with the LED indication on the Telindus 1031 Router itself. Refer to 2.6 - The front panel LED indicators on page 24 for more information on the interpretation of the LEDs.</td></tr>
<tr><td>interfaces</td><td>This reflects the status of the interfaces. The possible indications are:

<table><tr><th>Colour</th><th>Explanation</th></tr><tr><td>green</td><td>There is no alarm active in the corresponding interface object.</td></tr><tr><td>red</td><td>An alarm is active in the corresponding interface object.</td></tr></table>

The colours of the interfaces only change if the alarms related to the interface object are set to enabled in the alarmMask.</td></tr>
</table>

15 Auto installing the Telindus 1031 Router

Auto install includes a number of features that allow you to partially or completely configure the Telindus 1031 Router without on-site intervention.

The following gives an overview of this chapter:

- 15.1 - What is BootP and DHCP? on page 342
- 15.2 - Getting the LAN IP address on page 343
- 15.3 - Getting the configuration with TFTP on page 344
- 15.4 - Creating configuration files on page 347
- 15.5 - Creating a binary configuration file on page 348
- 15.6 - Creating an ASCII configuration file on page 349

15.1 What is BootP and DHCP?

BootP and DHCP are very similar protocols. IP devices without IP address use them to obtain an IP address.

Compliance:

- BootP complies with RFC951.
- DHCP complies with RFC2131 and RFC2132.

In both protocols, the client IP device sends a limited broadcast request on its interfaces requesting an IP address. The request contains the client its MAC address, which is a unique identifier (refer to What is the ARP cache? on page 179 for more information).

BootP

A workstation with a BootP server interprets incoming BootP requests. You can configure a file on the server with MAC address and IP address/subnet mask pairs for all devices in the network you want to service. If the MAC address in the BootP request matches a MAC address in this file, the BootP server replies with the corresponding IP address and subnet mask.

Assigning an IP address in this way is done through a simple request - response handshake.

The Telindus 1031 Router, being a router, always requests a static IP address.

DHCP

A workstation with a DHCP server works in a similar way as with a BootP server. The difference with BootP is that you can additionally configure a list of IP addresses on the server. These IP addresses are dynamically assigned to the IP devices requesting an IP address, independently of their MAC address. Those address assignments are limited in time.

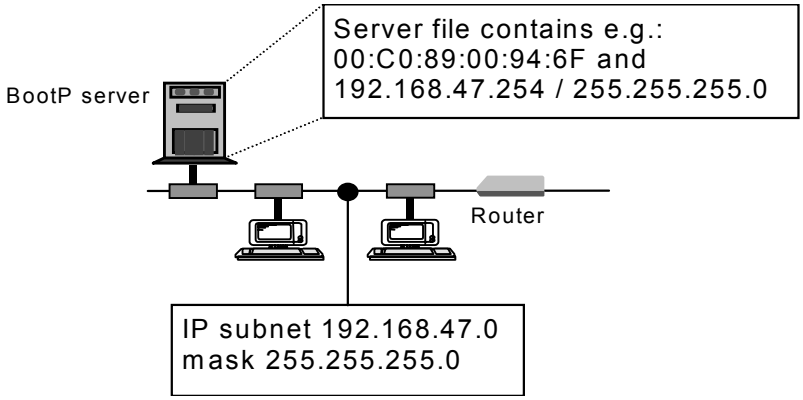
Assigning an IP address in this way is done through a 4-way handshake and with regular renewals.

The Telindus 1031 Router as relay agent

Being broadcast packets, BootP and DHCP requests can cross a router using IP helper addresses. The Telindus 1031 Router is a BootP and DHCP relay agent. This means it adds additional information to the request packets allowing servers on distant networks to send back the answer. This feature is not used in the auto install procedure.

15.2 Getting the LAN IP address

The following figure shows how the Telindus 1031 Router obtains its LAN IP address from a BootP server on its Ethernet interface:



The IP address is obtained as follows:

Phase	Description
1	In case on the LAN interface … • no IP address or subnet mask are configured (default value) AND the telindus1031/lanInterface/mode attribute is set to routing, OR • no IP address or subnet mask are configured (default value) AND the telindus1031/lanInterface/mode attribute is set to bridging (default value) AND no IP address or subnet mask are configured in the bridgeGroup (default value), … then the Telindus 1031 Router starts sending BootP requests every 10 seconds on its LAN interface. These requests contain the Telindus 1031 Router its MAC address.
2	The BootP server looks in its MAC address - IP address file. If the MAC address in the BootP request matches a MAC address in this file, the BootP server replies with the corresponding IP address and subnet mask. **Example** In the example above, the Telindus 1031 Router its MAC address is 00:C0:89:00:94:6F. The server replies with IP address 192.168.47.254 and corresponding subnet mask 255.255.255.0.
3	The Telindus 1031 Router uses this received IP address as its LAN IP address. It is stored in the Telindus 1031 Router its volatile memory. This means that after a cold boot, the Telindus 1031 Router has to request the LAN IP address again.

15.3 Getting the configuration with TFTP

Once the Telindus 1031 Router has obtained an IP address, it is reachable over its LAN interface. Now you can start a TMA or a Telnet session on the Telindus 1031 Router and configure it.

Alternatively the Telindus 1031 Router can retrieve its complete configuration without any user intervention. As long as the previously obtained IP addresses are not stored in non-volatile memory, the Telindus 1031 Router tries to get a complete configuration file from a TFTP server.

The configuration file and TFTP

The Trivial File Transfer Protocol is typically used in combination with BootP to obtain the configuration of a device from a TFTP server. The configuration file on this TFTP can be in a binary or an ASCII format. How to build such files is explained in 15.4 - Creating configuration files on page 347.

Getting the configuration file with TFTP

The Telindus 1031 Router asks for its configuration file as follows:

Phase	Description
1	The Telindus 1031 Router sends a DNS request on the interface for which it received an IP address. This request is a local broadcast message. If it sent over the WAN link, the peer router should have an IP helper address for the DNS server. If no reply is received within 10 seconds, this phase is repeated once more.
2	If a DNS reply is received, it contains the domain name. The Telindus 1031 Router only uses the hostname part of the domain name: *hostname.domain.toplevel_domain*.

<table>
<tr><th>Phase</th><th>Description</th></tr>
<tr><td>3</td><td>Now there are two possibilities:
<table>
<tr><th>If the host name is …</th><th>then …</th></tr>
<tr><td>known,</td><td>the router requests the file hostname.cms as a limited broadcast. hostname.cms is the router its configuration file in binary format.

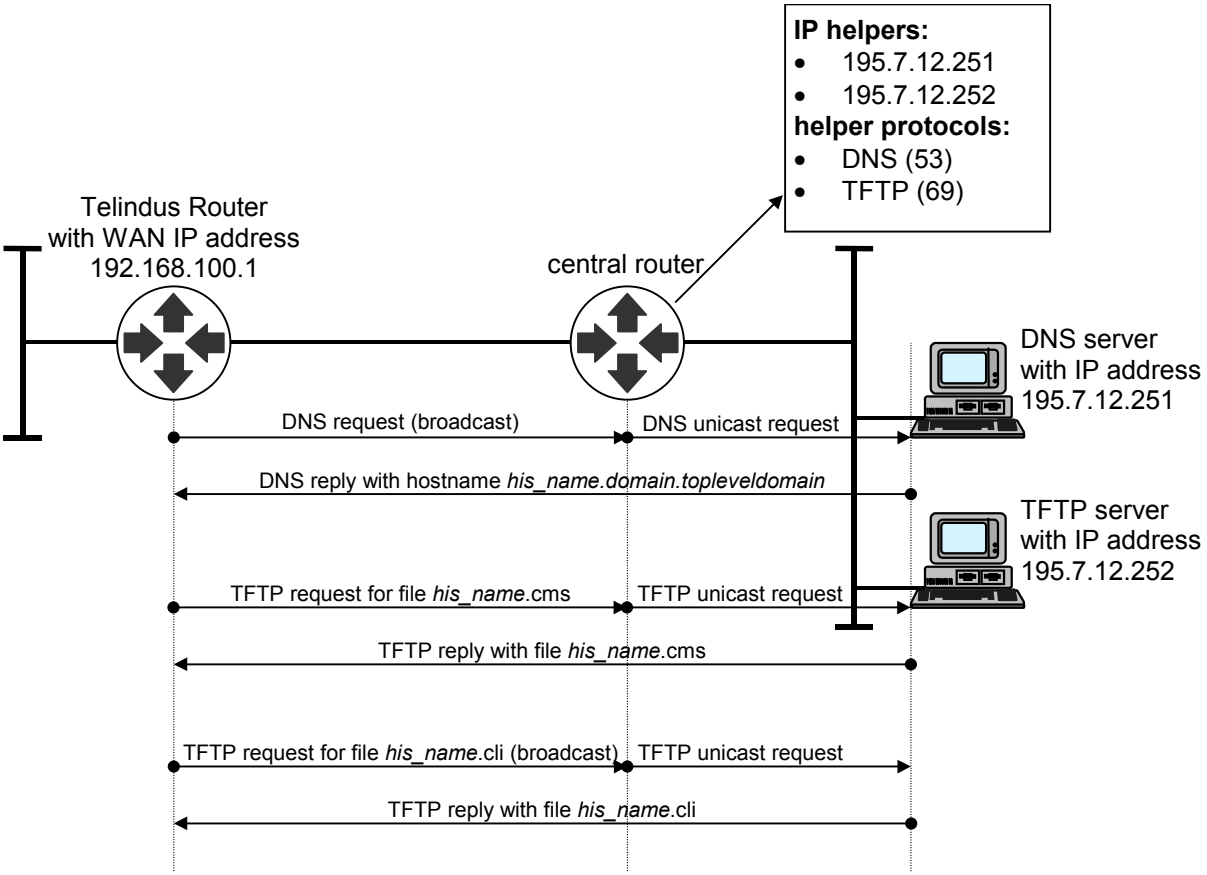
If this request is sent over the WAN link, the peer router should have an IP helper address for the TFTP server.

If no reply is received within 5 seconds, the router requests the file hostname.cli as a local broadcast. hostname.cli is the router its configuration file in ASCII format. Again there is a reply time-out of 5 seconds.

If still no valid answer is received, the router alternatively repeats both requests up to four times.</td></tr>
<tr><td>not known,</td><td>the procedure described above is executed with the file name hostname replaced by the concatenation of the decimal representation for each byte in the IP address, with leading zeroes and without dots in between the bytes.

Example, a router with IP address 192.168.100.1 requests the file 192168100001.cms or 192168100001.cli.</td></tr>
</table></td></tr>
<tr><td>4</td><td>If the Telindus 1031 Router received a valid configuration file, then it stores the configuration and possibly reboots. Else it restarts with phase 1.</td></tr>
</table>

The following figure illustrates the procedure as described in the table above. It shows the procedure over a WAN link. The IP address of the router is 192.168.100.1 and its hostname is *his_name*. In this example, the DNS server and TFTP server are on different machines. However, in reality these two services often reside on the same machine.



15.4 Creating configuration files

In 15.3 - Getting the configuration with TFTP on page 344, you have seen how you can get a configuration file with TFTP. The two possible configuration file formats used by TFTP are:

File type	Extension	How to create the configuration file
binary	.cms	Use the TMA export utility and choose the CMS file type. This is the most compact format. Refer to 15.5 - Creating a binary configuration file on page 348.
ASCII	.cli	Use the CLI user interface. Refer to 15.6 - Creating an ASCII configuration file on page 349. When you download an ASCII (*.cli) configuration file to the Telindus 1031 Router, make sure that each line in this file contains no more than 500 characters.

15.5 Creating a binary configuration file

To create a configuration file in binary (*.cms) format, proceed as follows:

Step	Action
1	Start a TMA session on the Telindus 1031 Router.
2	Make changes to its configuration (if necessary) in order to obtain the desired configuration. You do not have to send these configuration changes to the Telindus 1031 Router.
3	Click on the *Export data to file* button: .
4	In the *Export configuration parameters* window, select the following: • Choose a directory where to save the file. • Enter a name for the file. • Make sure the file type is CMS. • Make sure the *Full configuration* option is selected.
5	Click on the *Save* button. The edited configuration of the Telindus 1031 Router is stored on the PC in binary format. The file contains the complete configuration including the *Activate Configuration* command. As a result, the configuration is immediately activated when downloaded with TFTP.

15.6 Creating an ASCII configuration file

To create a configuration file in ASCII format, you can use the CLI syntax as explained in the Maintenance Tools manual. However, for the first time user it is easier to retrieve the configuration in the CLI format from the Telindus 1031 Router.

There are two possible ways to create a configuration file in ASCII (*.cli) format:

- 15.6.1 - Creating an ASCII file using the TFTP get command on page 350
- 15.6.2 - Creating an ASCII file using the CLI get command on page 351

Do not use the TMA export utility for creating an ASCII type configuration file (not even when saving it as a TXT file). The resulting format is not compatible with the CLI format.

15.6.1 Creating an ASCII file using the TFTP *get* command

To create a configuration file in ASCII (*.cli) format using the TFTP *get* command, proceed as follows:

Step	Action
1	Start a TFTP session on the Telindus 1031 Router. For example by typing `tftp 10.0.11.1` at the command prompt of your UNIX station, where 10.0.11.1 is the LAN IP address of the Telindus 1031 Router.
2	Get the configuration file of the Telindus 1031 Router. **Example** `tftp> get CONFIG.CLI dest_file.cli` Where … • `get` is the TFTP command to retrieve a file, • `CONFIG.CLI` is the Telindus 1031 Router configuration file, • `dest_file.cli` is the destination file.
3	When the file transfer is finished, close the TFTP session.

15.6.2 Creating an ASCII file using the CLI *get* command

To create a configuration file in ASCII (*.cli) format using the CLI *get* command and Telnet logging, proceed as follows:

Step	Action
1	Start a Telnet session on the Telindus 1031 Router. You are automatically in CLI mode.
2	Redirect the CLI output or log it to a file.
3	Make sure you are in the top object (telindus1031) and in the "Edit Configuration" group.
4	Execute the `get -r` command.
5	Stop output redirection or logging.
6	In the redirected or logged file you now obtained, remove all input and output logging before the *get -r* command. Also remove the *get -r* command itself.
7	Now, modify the configuration file: **Step** / **Action** 1 – Change the string *GET*, now located at the beginning of the file, into *SET*. 2 – Type the string *Load Default Configuration* at the beginning of the file. 3 – Type the string *Activate Configuration* at the end of the file.
8	Save this file to a file with an extension **.cli*.

16 Downloading software

This chapter explains how to download loader software in the memory and application software to the file system of the Telindus 1031 Router. It also shows how to download any other file to the file system of the Telindus 1031 Router. But first it explains the difference between boot, loader and application software.

The following gives an overview of this chapter:

- 16.1 - What is boot, loader and application software? on page 354
- 16.2 - Downloading application software using TMA on page 355
- 16.3 - Downloading application software using TFTP on page 356
- 16.4 - Downloading application or loader software using TML on page 357
- 16.5 - Downloading application or loader software in loader mode on page 358
- 16.6 - Downloading files to the file system on page 359

16.1 What is boot, loader and application software?

What is boot software?

The boot software takes care of the initial phase in the start-up sequence of the Telindus 1031 Router. It is located on the lowest software level.

What is loader software?

The boot software takes care of the second phase in the start-up sequence of the Telindus 1031 Router. It is located on the middle software level.

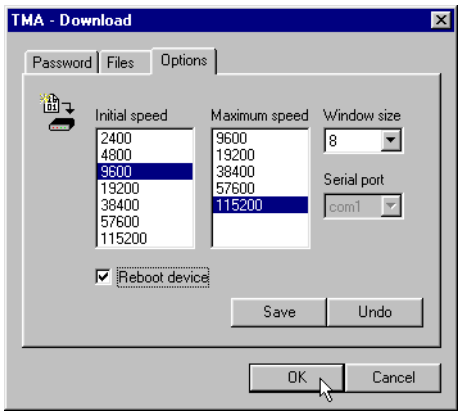
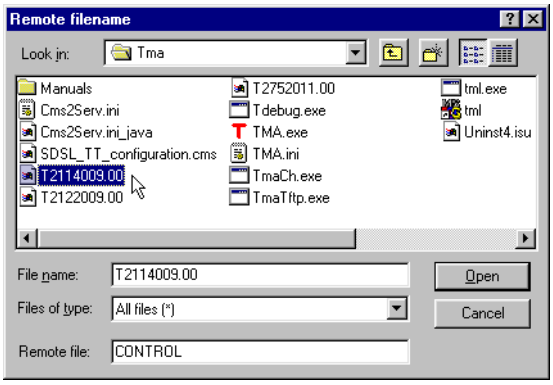
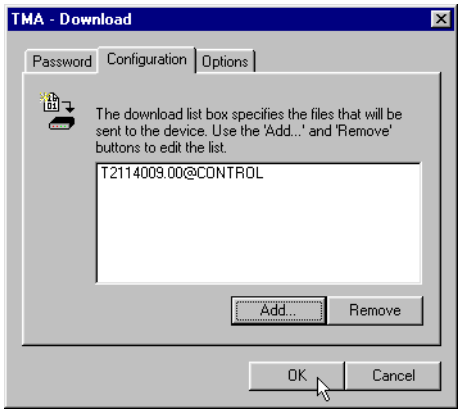
As opposed to boot mode, you can force the Telindus 1031 Router to run in loader mode. In this mode you can then download new loader or application software. This may be necessary in case a software download failed or a flash memory error occurred making the Telindus 1031 Router inaccessible or even inoperative.

What is application software?

The application software, also called control software or firmware, completely controls the Telindus 1031 Router. It is located on the highest software level.

16.2 Downloading application software using TMA

To download application software to the Telindus 1031 Router using TMA, proceed as follows:

Step	Action
1	Establish a link between TMA and the Telindus 1031 Router either over a serial or an IP connection. Refer to 4 - Managing the Telindus 1031 Router on page 33.
2	In the TMA window select *Tools* → *Download…*
3	In case you made … • an IP connection, skip this step. • a serial connection, select the *Options* tab in the *TMA - Download* window. Then set the following: - Set the initial transfer speed to 9600 bps. - If you set the maximum transfer speed to 115200 bps, the actual transfer speed will be negotiated between 9600 bps and 115200 bps. 
4	In the *TMA - Download* window, select the *Configuration* tab and click on *Add…*
5	In the *Remote filename* window, do the following: 1. Select the file you want to download (e.g. T1234001.00). 2. Type CONTROL in the *Remote file* field. 3. Click on *Open*. 
6	If you are currently connected to the Telindus 1031 Router without write access, then you can enter a password in the *Password* tab which gives you write access. Else leave the *Password* tab blank.
7	When the *TMA - Download* window reappears, click on *OK*. ⇒A window opens and shows the download progress. 

16.3 Downloading application software using TFTP

When downloading with TMA over an IP connection, you actually evoke TFTP (Trivial File Transfer Protocol) through TMA. You can also use TFTP without opening TMA.

To download application software to the Telindus 1031 Router using TFTP, proceed as follows:

Step	Action
1	Start a TFTP session on the Telindus 1031 Router. For example by typing `tftp 10.0.11.1` at the command prompt of your computer, where 10.0.11.1 is the LAN IP address of the Telindus 1031 Router.
2	Set the following TFTP parameters: • Set the retransmission time-out to at least 20 seconds. The syntax to do this is typically `rexmt 20`. • Set the total TFTP time-out sufficiently large (e.g. 40 seconds). The syntax to do this is typically `timeout 40`. • Set the transfer mode to binary (octet) format. The syntax to do this is typically `binary` or `octet`.
3	Type the following command: `tftp> put Txxxxxxx.00@CONTROL?my_pwd` Where … • `put` is the TFTP command to send a file. • `Txxxxxxx.00` is the application software file (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the file being downloaded is an application software file. • `?my_pwd` is the write access password as configured in the Telindus 1031 Router. If no password has been configured, you may omit the ? and the password.
4	When the file transfer is finished, close the TFTP session.

16.4 Downloading application or loader software using TML

When downloading with TMA over a serial connection, you actually evoke TML (Telindus Memory Loader) through TMA. You can also use TML without opening TMA.

To download application or loader software to the Telindus 1031 Router using TML, proceed as follows:

Step	Action
1	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the control connector of the Telindus 1031 Router.
2	Open a DOS window on your computer.
3	Go to the directory where the TML executable is located. Typically this is *C:\Program Files\TMA*.
4	Place the software file you want to download in this directory.
5	Type the following command: `tml -c1 -v -b -fTxxxxxxx.00@CONTROL?my_pwd` where … • `tml` is the executable (Telindus Memory Loader) to download files to the Telindus devices through their control port. • `-c1` specifies the COM port of the computer connected to the Telindus 1031 Router (in this example COM1). • `-v` returns graphical information on the download status. • `-b` puts the Telindus 1031 Router in boot mode. This is only necessary when you want to download loader software. • `-fTxxxxxxx.00` is the software file you want to download (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the file being downloaded is an application or loader software file. • `?my_pwd` is the write access password as configured in the Telindus 1031 Router. If no password has been configured, you may omit the ? and the password. To see a list of all the possible TML options: type `TML` in your DOS windows and press the ENTER key.
6	If you press the ENTER key, the software download begins. If you used the *-v* option together with the TML command, a graphical bar shows the download progress.

16.5 Downloading application or loader software in loader mode

When a loader or application software download failed or when a flash memory error occurs, it may be possible that the Telindus 1031 Router becomes inaccessible or even inoperative. In that case, new software can still be downloaded by forcing the Telindus 1031 Router in loader mode. Do this by means of the *loader mode* DIP switch. Refer to 3.2 - DIP switches of the Telindus 1031 Router on page 31.

To download loader or application software to a Telindus 1031 Router in loader mode, proceed as follows:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 32.
2	Set DIP switch bank DS2 position 1 to *off*. Refer to 3.1 - The Telindus 1031 Router motherboard on page 30 to locate this DIP switch bank.
3	Replace the cover without fastening the screws and reconnect the power supply. ⇒The Telindus 1031 Router reboots in loader mode.
4	Now proceed as explained in the previous section, 16.4 - Downloading application or loader software using TML on page 357.
5	When the software download is finished, again disconnect the power supply and open the housing.
6	Reset DIP switch bank DS2 position 1 to *on*.
7	Properly replace the cover as described in 3.3 - Opening and closing the housing on page 32 and reconnect the power supply.

16.6 Downloading files to the file system

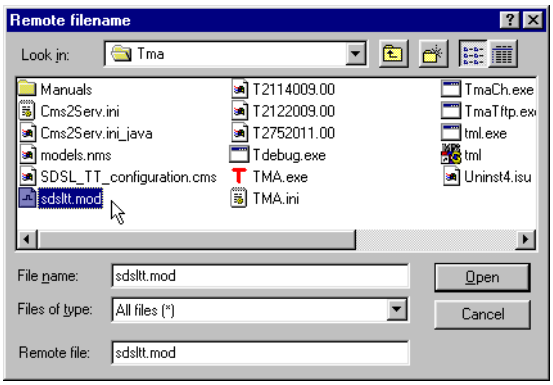
When you use the proxy function of the Telindus 1031 Router, you may need to download certain files to the file system of the Telindus 1031 Router. For example …

- model files in case you want to manage the network units that are connected to the Telindus 1031 Router with a management application that requires these (e.g. ATWIN, CLI, Web Interface, etc.).
- configuration files of network units for the purpose of configuration consistency / distribution.
- application software of network units for the purpose of software consistency / distribution.
- etc.

In fact, any file can be downloaded to the file system of the Telindus 1031 Router. You can do this using the same tools you use to download application software. These tools are:

- TMA (refer to 16.2 - Downloading application software using TMA on page 355).
- TFTP (refer to 16.3 - Downloading application software using TFTP on page 356).
- TML (refer to 16.4 - Downloading application or loader software using TML on page 357).

The major difference is that instead of specifying CONTROL as target filename for the application software, you now can specify any filename as target filename.

Tool	Example
TMA	In the *Remote filename* window, do the following: 1. Select the file you want to download (e.g. *sdsltt.mod*). 2. Type the target filename in the *Remote file* field (e.g. *sdsltt.mod*). 3. Click on *Open*. 
TFTP and TML	• `tftp> put filename1.ext@filename2.ext?my_pwd` • `tml -c1 -v -ffilename1.ext@filename2.ext?my_pwd` Where … • `filename1.ext` is the source filename. This is a file on your computer. • `filename2.ext` is the target filename. This is the filename the source file will get when it is placed on the file system. Source and target filename may be the same, but if wanted, you may specify a different target filename. Example: • `tftp> put models.nms@models.nms?pwd123` • `tml -c1 -v -fmodels.nms@models.nms?pwd123`

17 Technical specifications

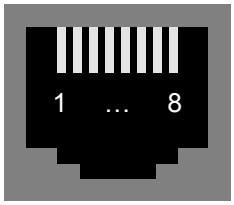
This chapter gives the technical specifications of the Telindus 1031 Router. The following gives an overview of this chapter:

- 17.1 - G703 interface specifications on page 362
- 17.2 - LAN interface specifications on page 363
- 17.3 - Control connector specifications on page 364
- 17.4 - Auxiliary connector specifications on page 365
- 17.5 - ATM encapsulation specifications on page 366
- 17.6 - Frame Relay encapsulation specifications on page 366
- 17.7 - PPP encapsulation specifications on page 366
- 17.8 - IP routing specifications on page 367
- 17.9 - Bridging specifications on page 367
- 17.10 - Routing and bridging performance specifications on page 367
- 17.11 - Power requirements on page 368
- 17.12 - Dimensions on page 368
- 17.13 - Safety compliance on page 368
- 17.14 - Over-voltage and over-current protection compliance on page 368
- 17.15 - EMC compliance on page 368
- 17.16 - Environmental compliance on page 369

17.1 G703 interface specifications

- Connector: RJ45
- Compliance: ITU-T G.703
- Coding: AMI or HDB3 (configurable)
- Speed: 2 Mbps
- Framing: framed or unframed (configurable), framing compliant to G.704
- Time slots: N x 64 kbps (N = 1 … 32)
- CRC4 insertion: enabled, disabled or automatic detection (configurable)
- Performance monitoring: compliant to G.826
- Jitter and wander: compliant to G.823

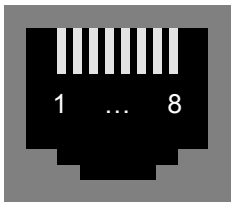
The following table shows the connector layout of the RJ45 G703 interface connector:

Pin	Signal	DTE	Figure
1	receive A	input	
2	receive B	input	
3	shielding ground	-	
4	transmit A	output	
5	transmit B	output	
6	shielding ground	-	
7	not connected	-	
8	not connected	-	

17.2 LAN interface specifications

- Applicable standards: IEEE 802.3 (10Mbps Ethernet), IEEE 802.3u (100Mbps Ethernet)
- 10/100Mbps auto-sense
- Connector: RJ45 Unshielded Twisted Pair (UTP)

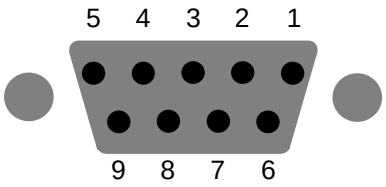
The following table shows the connector layout of the RJ45 Ethernet LAN interface connector:

Pin	Signal	I/O	Figure
1	transmit (positive)	output	
2	transmit (negative)	output	
3	receive (positive)	input	
4	not used	-	
5	not used	-	
6	receive (negative)	input	
7	not used	-	
8	not used	-	

17.3 Control connector specifications

The control connector (sometimes also called NMS port) is a 9 pins subD connector labelled CTRL. The signals on these connector are V.24 / V.28 signals.

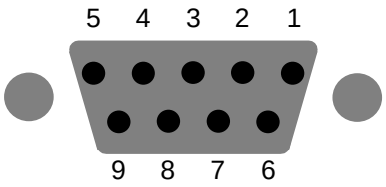
The control connector has the following pin layout:

Pin	Signal		DCE	Figure
1	not used	-	-	
2	Receive Data	RxD	output	
3	Transmit Data	TxD	input	
4	not used	-	-	
5	GND	GND	-	
6	not used	-	-	
7	not used	-	-	
8	not used	-	-	
9	not used	-	-	

17.4 Auxiliary connector specifications

The auxiliary connector is a 9 pins subD connector labelled AUX. The signals on these connector are V.24 / V.28 signals.

The control connector has the following pin layout:

Pin	Signal		DCE	Figure
1	Data Carrier Detect	DCD	input	
2	Receive Data	RxD	input	
3	Transmit Data	TxD	output	
4	Data Terminal Ready	DTR	output	
5	signal ground	GND	-	
6	Data Set Ready	DSR	input	
7	Request To Send	RTS	output	
8	Clear To Send	CTS	input	
9	Ring Indicator	RI	input	

17.5 ATM encapsulation specifications

- ATM cell format ITU-T I.361
- ATM forum UNI 3.1/4.0 PVCs
- ATM forum ILMI 3.1/4.0
- OAM F5 loopback support (ITU-T I.610)
- Supports up to 8 ATM PVCs
- Supports ATM Forum Traffic Management 4.0 service types CBR and UBR

ATM AAL5 encapsulation

- RFC1483, RFC2684
- PPPoA (RFC2364)
- PPPoE (RFC2516)

17.6 Frame Relay encapsulation specifications

- Encapsulation compliant with RFC1490, RFC2427
- Support of multiple DLCI's (PVC)
- CIR (Committed Information Rate) configurable per DLCI
- Support of Reverse ARP over Frame-Relay for automatic gateway configuration
- EIR (Excess Information Rate) configurable per DLCI
- Support of LMI (revision 1 LMI, ANSI T1.617 and ITU-T)

17.7 PPP encapsulation specifications

- Encapsulation compliant with RFC1661, RFC1662
- IPCP (RFC1332)
- BCP (RFC2878)
- Support of CHAP authentication with MD5 hashing (RFC1994)

17.8 IP routing specifications

- IP (RFC791)
- ARP (RFC826)
- Static routing, RIP1 (RFC1058), RIP2 with MD5 hashing and authentication (RFC2453)
- Router requirements (RFC1812)
- Standard and extended access filtering on LAN and WAN interfaces
- NAT (Network Address Translation) with dynamic or static IP address conversion and PAT (Port Address Translation) (RFC3022)
- BOOTP/DHCP server, relay agent (RFC2131, RFC2132)
- BOOTP client (RFC951)
- Numbered/unnumbered WAN Interface
- DiffServ priority tagging and queuing (RFC2474, RFC2475)
- L2TP tunnelling (RFC2661) on WAN and LAN interfaces

17.9 Bridging specifications

- Bridging with spanning tree protocol (IEEE 802.1D)
- VLAN interconnect (IEEE 802.1Q)
- Integrated Routing and Bridging (IRB)

17.10 Routing and bridging performance specifications

- Full forwarding performance of 64 byte packets at 10 Mbps
- Buffering: up to 4800 packets (64 bytes/packet)

17.11 Power requirements

- 9 Vdc ±10%, 500 mA
- External power adapters available for 48Vdc and 230 Vac

17.12 Dimensions

- Height: 45 mm
- Width: 220 mm
- Depth: 235 mm
- Weight: 700 g

17.13 Safety compliance

- EN60950
- Class 1 equipment for Table Tops with 115/230 Vac internal power supply.
- Class 3 equipment for …
  - Table Tops with 115/230 Vac external power supply adapter
  - Table Tops with -48 Vdc internal power supply
  - Card Versions.

17.14 Over-voltage and over-current protection compliance

The over-voltage and over-current protection complies with ITU-T K.44 and ETSI ETS 300 386-2 recommendations.

17.15 EMC compliance

- EN55022 B Emissions
- EN55024 Immunity
- EN61000-3-2 Harmonics
- EN61000-3-3 Voltage fluctuations and flicker
- EN61000-4-2 ESD
- EN61000-4-3 Radiated immunity
- EN61000-4-4 EFT/burst
- EN61000-4-5 Surge
- EN61000-4-6 Conducted immunity
- EN61000-4-8 Power magnetic field immunity
- EN61000-4-11 Voltage dips & drops
- ENV50204 Radiated immunity against digital radio telephone

17.16 Environmental compliance

- Storage conditions: ETSI ETS 300 019-1-1 Class 1.1. In addition, the storage temperature has to be between -25 to +70°C
- Transport conditions : ETSI ETS 300 019-1-2 Class 2.3
- Stationary use conditions: ETSI ETS 300 019-1-3 Class 3.2. In addition, the requirements below apply:
  - relative humidity 5 to 95% non-condensing and ambient operational temperature -5 to 45°C
    or
  - relative humidity 0 to 95% non-condensing and ambient operational temperature -10 to 50°C
- Maximum altitude: 3000m
- International protection (IP) class of protection against solid and liquids: IP40

Annex

Annex A: common TCP and UDP numbers

The following table shows the port numbers for a number of common protocols using TCP and UDP as transport protocol. As far as possible, the same port numbers are used for TCP as for UDP. A complete list can be found in the RFCs (Requests For Comment).

Port No	Protocol	UDP/TCP	Description
20	ftp-data	TCP	File Transfer (Default Data)
21	ftp	TCP	File Transfer (Control)
23	telnet	TCP	Telnet
25	smtp	TCP	Simple Mail Transfer Protocol
37	time	UDP/TCP	Time Server
42	nameserver	UDP	Host Name Server
53	domain	UDP/TCP	Domain Name Server
65	tacacs-ds	UDP/TCP	TACACS-Database Service
67	bootps	UDP	Bootstrap Protocol Server
68	bootpc	UDP	Bootstrap Protocol Client
69	tftp	UDP	Trivial File Transfer
80	www-http	TCP	World Wide Web HTTP
119	nntp	TCP	Network News Transfer Protocol
137	netbios-ns	UDP	NETBIOS Name Service
138	netbios-dgm	UDP	NETBIOS Datagram Service
139	netbios-ssn	UDP	NETBIOS Session Service
161	snmp	UDP	SNMP
162	snmptrap	UDP	SNMPTRAP
1728	telindus	UDP	Telindus Protocol used by TMA

Annex B: product information

The following table displays the product information of the Telindus 1031 Router:

Sales code	Product name	Description
177460	TELINDUS 1031 ROUTER 230VAC	IP router and bridge with 1 10/100Mbit/s Ethernet interface and 1 2Mbit/s G.703 interface. Includes European 230VAC power adapter.
177461	TELINDUS 1031 ROUTER NPWR	IP router and bridge with 1 10/100Mbit/s Ethernet interface and 1 2Mbit/s G.703 interface. Delivered without power adapter.
177485	USER AND REFERENCE MANUAL TELINDUS 1030 SERIES ROUTER	User and Reference manual for the Telindus 1030 router series. The Orchid functionality is not included in this manual.
177486	USER AND REFERENCE MANUAL TELINDUS 1030 SERIES ORCHID	User and Reference manual for the Orchid functionality on the Telindus 1030 router series. This includes the specific Orchid functionality on the whole series when it is activated as well as the specific features on the 1035 model.
171304	PWR-PLUG 48VDC->7,5VDC	48VDC wall plug power module for Desktop units delivered without external power plug
175592	PWR-PLUG (UK VERSION) 230VAC->9VDC	Wall plug power module for Desktop units delivered without external power plug. UK version
175590	PWR-PLUG (EUR VERSION) 230VAC->9VDC	Wall plug power module for Desktop units delivered without external power plug. EUR version

Index

A

absolute and relative addressing 240

action, what is 43

activating the configuration 68

adding an object to the containment tree 45
- how 47
- in (TMA) CLI 47
- in ATWIN 47
- in the Web Interface 48
- in TMA 47
- referring to the added object 49
- when 46
- which objects 46
- why 46

address translation
- basic configuration 116

addressing, relative and absolute 240

alarm attributes 327
- configuration 330
- general 331
- introduction 329
- overview 328

alarms
- G703 channel 336
- G703 interface 335
- general 332
- LAN interface 334
- router 337

application software
- downloading
  - using TFTP 356
  - using TMA 355
  - using TML 357
- version iv
- what is 354

ARP cache
- how works the 179
- time-out 179
- what is 179

ATM
- basic configuration 86
- configuration attributes 193
- introducing 87
- performance attributes 311
- specifications 366
- status attributes 270
- what is 87

ATM layers, what are 88

ATM switching, how works 87

attribute
- overview 50
- what is 42

attribute - action
- Activate Configuration 68, 176
- clearArpCache 256, 292
- clearBridgeCache 292
- Cold Boot 177
- Delete File 295
- Load Default Configuration 68, 176
- Load Saved Configuration 68, 176
- Rename File 295
- resetNat 316
- startPing 314
- stopPing 314

attribute - alarm
- alarmInfo 331
- alarmLevel 330
- alarmMask 330
- totalAlarmLevel 331

attribute - configuration
- accessList 241
- adapter 180
- addresses 216
- alarmFilter 243
- alarmLevel
  - lanInterface object 180
  - router object 214
  - top object 176
  - wanInterface object 184
- alarmMask
  - lanInterface object 180
  - router object 214
  - top object 176
  - wanInterface object 184
- algorithm 228
- alternativeRoutes 204
- arp 179, 233
- atmConfig 198
- authenPeriod 187
- authentication 187
- bootFromFlash 174
- bridgeCache 232
- bridgeTimeOut 232
- bridging 180, 185, 199
- clocking 182
- cms2Address 240
- coding 182
- consoleNoTrafficTimeOut 242
- countingPolicy 230
- crc4Insertion 183
- ctrlPortProtocol 242
- defaultRoute 201
- dhcpCheckAddress 214
- dhcpDynamic 212
- dhcpStatic 211
- dlciTable 189
- dmzHost 217
- dropLevels 226
- encapsulation 184
- filter 222
- framing 182
- gateway 216
- helperProtocols 208
- ip 178, 185, 188, 233
- ipAddress (loopback) 243
- jitterAttenuation 183
- l2tpTunnels 218
- linkMonitoring 186
- lmi 191
- longHaul 183
- lowdelayQuotum 230
- macAddress 236
- maxFifoQLen 184
- method 223
- mib2Traps 239
- mode 180, 185
- name 178, 233
- patAddress 215
- portTranslations 215
- pppSecretTable 207
- priorityPolicy 184
- pvcTable 193
- queueConfigurations 230
- ripHoldDownTime 205
- ripUpdateInterval 204
- ripv2SecretTable 206
- routingProtocol 203
- routingTable 202
- security 175
- sendAdminUnreachable 210
- sendPortUnreachable 210
- sendTtlExceeded 209
- servicesAvailable 216
- snmp 242
- spanningTree 234
- sysContact 174
- sysLocation 174
- sysName 174
- sysSecret 207
- tcpSockets 217
- tcpSocketTimeOut 217
- telnet 242
- tftp 242
- timeSlots 184
- tos2QueueMapping 227
- trafficShaping 224
- trapDestinations 238
- udpSockets 217

udpSocketTimeOut 217
vlan 235
vlanPriorityMap 237
attribute - performance
addressesAvailable 315
allocFails 315
bridgeAccessList 320
bridgeCache 319
bridgeDiscards 319
bridgeFloods 319
cliSessionCount 321
cllmInFrames 310
cms2SessionCount 321
currUsedProcPower 323
discards 315
dlciTable 308
errorCount 306
freeBlockCount 323
freeDataBuffers 323
freeMemory 324
h24Performance 304
h2Performance 304
icmpAllocs 316
icmpSocketsUsed 315
ifInDiscards 302
ifInErrors 302
ifInNUcastPkts 302
ifInOctets 302
ifInUcastPkts 302
ifInUnknownProtos 302
ifOutDiscards 303
ifOutErrors 303
ifOutNUcastPkts 303
ifOutOctets 302
ifOutPQLen 307
ifOutQLen 303
ifOutUcastPkts 302
l2tpTunnels 317
largestFreeBlockSize 323
lmi 310
pingResults 314
pvcTable 311
routingTable 313
socketsFree 315
taskInfo 324
tcpAllocs 316
tcpSessionCount 322
tcpSocketsUsed 315
tftpSessionCount 321
totalDataBuffers 323
totalMemory 324
udpAllocs 316
udpSocketsUsed 315
unknownCells 311
usedProcPower 323
attribute - status
activeFlash 249
adapter 256
addresses 280
ais 258
arpCache 253, 288
atmSync 270
bcpHisOptions 264
bcpMyOptions 264
bcpState 261
bootVersion 249
bridgeCache 289
bridging 254, 265, 272, 290
cllmLastCongestionCause 269
cms2Address 293
coding 258
configurationSaving 250
corruptBlocks 294
deviceId 250
dhcpBinding 279
dhcpStatistics 279
dlciTable 266
fileList 294
flash1Version 249
flash2Version 249
flashVersions 249
freeSpace 294
hisAuthenstate 265
ifDescr 251, 258, 259, 287, 293
ifLastChange 251, 259
ifMtu 251, 259, 287, 293
ifOperStatus 251, 258, 260, 287, 293
ifSpeed 251, 258, 259
ifType 251, 258, 259, 287, 293
igmpTable 277
ip 252, 261, 266, 287
ipAddress 293
ipAdEntBcastAddr 256
ipAdEntReasmMaxSize 256
ipcpHisOptions 263
ipcpMyOptions 263
ipcpState 261
l2tpTunnels 281
lcpHisOptions 262
lcpMyOptions 262
lcpState 261
lfa 258
lmi 268
loaderVersion 249
los 258
macAddress 252
messages 250
myAuthenstate 265
openCircuit 258
pvcTable 270
routingTable 274
rxLevel 258
spanningTree 290
status 294
sysDescr 248
sysObjectID 248
sysServices 248
sysUpTime 248
taskInfo 296
auto install 341
auxiliary connector specifications 365

B

basic configuration 51
address translation 116
ATM 86
bridge 139
CIR 85
Classical IP 94
DLCI 83
extended access list 138
Frame Relay 77
G703 interface 61
HDLC 95, 96
IP addresses 55
on the ATM WAN 89
on the Frame Relay WAN 80
on the PPP WAN 75
L2TP tunnel 127
link monitoring 75
LMI 84
major features of the device 65
multi-protocol over ATM 94
passwords 62
PCR 91
PPP 73
PPP authentication 76
PVC 90
RIP 107
router 97
static routes 100
traffic and priority policy
on routed and bridged data 132
on the bridge 154
on the router 130
WAN encapsulation 71
BCP, what is 74
boot software, what is 354
BootP
relay agent 342
what is 342
BootP and DHCP, what are 342

BootP request, DHCP server reaction on a 213
BootP versus DHCP, releasing IP addresses 213
bridge
basic configuration 139
configuration attributes 231
general configuration attributes 232
introduction 140
performance attributes 318
specifications 367
status attributes 287
bridge access list
configuration attributes 236
performance attributes 320
bridge cache
time-out 232
what is 232
bridge group
configuration attributes 232
performance attributes 319
bridge port
state transition diagram 144
states 144
bridge traffic policy
applying on an interface 157
configuration attributes 237
bridging
configuring 149
configuring an IP address 150
configuring the bridging parameters on the interfaces 151
enabling on the interfaces 150
explaining the bridging structure 152
selecting the bridging protocol 150
setting the bridge priority 150
versus routing 98
what is 140
bridging structure, explanation 152

C

CHAP
authentication in both directions 76
authentication in one direction 76
what is 74
child object, what is 42
CIR
basic configuration 85
what is 78
Classical IP, basic configuration 94
combining bridging and routing in a network, a configuration example 165
common TCP and UDP numbers 373
configuration
activating the 68
loading the default
using the action 68
using the DIP switch 69
loading the saved 68
configuration action
executing 66
what is 67
configuration alarm attributes 330
configuration attributes 171
ATM 193
bridge 231
bridge access list 236
bridge group 232
bridge traffic policy 237
default NAT 215
Frame Relay 188
G703 channel 184
G703 interface 182
general 174
HDLC 199
L2TP tunnel 218
LAN interface 178
loop-back 243
management 240
overview 172
PPP 185
priority policy 228
proxy 244
router 200
router, general 201
SNMP 238
traffic policy 223
WAN interface 181
configuration examples 159
configuration file
creating a 347
creating a binary 348
creating an ASCII 349
using CLI get 351
using TFTP get 350
getting with TFTP 344
configuration type
active 67
default 67
explaining the 67
non-active 67
what is 67
configuring a priority policy 135
configuring a traffic policy
on the bridge 156
on the router 134
connecting a LAN to the Internet using NAT and PAT, a configuration example 163
connecting the device 18
an example 22
connecting the different parts of the device 20
connecting two networks through a tunnel, a configuration example 166
connecting VLAN enabled switches over a WAN, a configuration example 168
connecting with TMA
over an IP network 38
through the control connector 36
containment tree
adding an object 45
of the device 44
terminology 42
what is 42
control connector specifications 364
conventions in this manual
graphical vi
typographical v
copyright notice ii
creating passwords in the security table 63

D

default NAT
configuration attributes 215
performance attributes 315
status attributes 280

default route, an example 103

DHCP
relay agent 342
what is 342

DHCP server reaction on a BootP request 213

DHCP versus BootP, releasing IP addresses 213

dimensions of the device 368

DIP switch table, reading a 53

DIP switches 29
opening and closing the housing 32
overview 31
position on the motherboard 30

directed broadcast, what is 59

Discard Eligible bit, what is 79

DLCI
basic configuration 83
what is 78

document
application software version described in this iv
conventions
graphical vi
typographical v
copyright notice ii
intended audience iv
organisation iv
properties ii
statements iii
your feedback iv

downloading application software
in loader mode 358
using TFTP 356
using TMA 355
using TML 357

downloading loader software
in loader mode 358
using TML 357

downloading software 353

E

EIR, what is 78

element, what is 43

EMC compliance 368

environmental compliance 369

examples 159
combining bridging and routing in a network 165
connecting a LAN to the Internet using NAT and PAT 163
connecting two networks through a tunnel 166
connecting VLAN enabled switches over a WAN 168
LAN extension over a Frame Relay network 161
LAN extension over a PDH/SDH network 160
LAN extension over an ATM network 162
using PAT over PPP with a minimum of official IP addresses 164

executing configuration actions 66

extended access list
basic configuration 138

F

feedback iv

file system
status attributes 294

Frame Relay
basic configuration 77
configuration attributes 188
introduction 78
performance attributes 308
specifications 366
status attributes 266
what is 78

G

G703 channel
alarms 336
configuration attributes 184
performance attributes 307
status attributes 259

G703 interface
alarms 335
basic configuration 61
configuration attributes 182
performance attributes 306
specifications 362
status attributes 258

general
alarm attributes 331
alarms 332
configuration attributes 174
status attributes 248

group, what is 43

H

HDLC
basic configuration 95, 96
configuration attributes 199
introducing 96
status attributes 272

housing, opening and closing 32

I

ICMP message
communication prohibited 210
port unreachable 210
TTL exceeded 209

ICMP redirect, what is 59

IGMP
topology 277
what is 277

index name, what is 42

installation and connection precautions 17

installing and connecting the device 13

introducing
alarm attributes 329
ATM 87
bridging 140
Frame Relay 78
HDLC 96
L2TP 128
management terminology 40
management tools 10
NAT 117
PAT 117
PPP 74
RIP 108
router applications 5
routing 98
the device 4
traffic and priority policy 131

introduction 3

IP addresses
automatically obtaining 56
basic configuration 55
on the ATM WAN 89
on the Frame Relay WAN 80
on the PPP WAN 75
explaining the IP structure 58
Frame Relay DLCI global IP 81
Frame Relay DLCI specific IP 82
getting the LAN IP address 343
where to find the IP related parameters 57
IP structure
explanation 58
where to find 57
IPCP, what is 74

L

L2TP
basic configuration 129
how works 129
introduction 128
terminology 128
what is 128
L2TP status
authentication states 286
call states 284
control states 283
delivery states 285
L2TP tunnel
basic configuration 127
configuration attributes 218
performance attributes 317
status attributes 281
LAN extension over a Frame Relay network, a configuration example 161
LAN extension over a PDH/SDH network, a configuration example 160
LAN extension over an ATM network, a configuration example 162
LAN interface
alarms 334
configuration attributes 178
performance attributes 302
specifications 363
status attributes 251
LCP, what is 74
LED indicators 24
G703 data LED 26
G703 link LED 26
introduction 25
LAN collision LED 27
LAN LED 26
power LED 26
states 25
link monitoring, basic configuration 75
LMI
basic configuration 84
what is 78
loader software
downloading using TML 357
what is 354
loading the default configuration
using the action 68
using the DIP switch 69
loading the saved configuration 68
loop-back
configuration attributes 243
status attributes 293

M

major features of the device, basic configuration of the 65
management
configuration attributes 240
performance attributes 321
status attributes 293
management terminology, introducing 40
management tools
connection possibilities 12
introducing 10
managing the device 33
with TMA 34
motherboard, position of the DIP switches 30
multi-protocol over ATM
basic configuration 94
what is 88

N

NAT
basic configuration 124
introduction 117
what is 117
when use 118
why use 117
NAT address table, how works the 125
NAT and PAT
combining 126
NAT on the LAN interface, a remark 124

O

OAM F5 loop-back cells, what are 197
object 183
object, what is 42
operating system
performance attributes 323
status attributes 296
organisation of this manual iv
overview
alarm attributes 328
configuration attributes 172
performance attributes 300
status attributes 246
over-voltage and over-current protection compliance 368

P

parent object, what is 42
parts of the device 20
passwords
basic configuration 62
correcting the security table 63
creating in the security table 63
entering in the different management tools 64
remarks on 175
PAT
introduction 117
limitations 122
limitations workaround 123
what is 117
when use 118
why use 117
PAT and NAT
combining 126

PCR
basic configuration 91
performance attributes 299
ATM 311
bridge 318
bridge access list 320
bridge group 319
default NAT 315
Frame Relay 308
G703 channel 307
G703 interface 306
L2TP tunnel 317
LAN interface 302
management 321
operating system 323
overview 300
proxy 325
router 312
router, general 313
WAN interface 305
policies on the bridge
basic configuration 154
policies on the router
basic configuration 130
power requirements 368
PPP
authentication, basic configuration 76
basic configuration 73
configuration attributes 185
handshake 74
introducing 74
specifications 366
status attributes 261
what is 74
priority policy
applying on an interface 137
configuration attributes 228
configuring 135
how to configure on the bridge 155
how to configure on the router 133
what is 131
priority queuing, what is 131
private IP address range 117
product information 375
proxy
configuration attributes 244
performance attributes 325
status attributes 297
PVC
basic configuration 90

R

reading a
DIP switch table 53
TMA attribute string 54
reading DIP switch tables and TMA attribute strings 52
rear view of the device 19
referring to an added object
example 49
how to 49
what is 49
relative and absolute addressing 240
releasing IP addresses, DHCP versus BootP 213
remarks on
ATM on G703 interface 61, 184, 193
bridging traffic policy on the LAN interface 157
CIR 85
dhcpStatistics attribute 279
G703 data LED 26
HDLC encapsulation 96
helperProtocols attribute 208
host routes to local interface IP address 276
ifOperStatus of the WAN interface 260
IP address on the LAN interface in case of bridging 57, 178, 233
messages attribute 250
natAddresses attribute 124
passwords 175
priority policy on the bridge 156
rerouting principle 106
resetNat action 316
rip2Authentication attribute 113
ripv2SecretTable attribute 206
routing traffic policy on the LAN interface 59, 136
rerouting principle, what is 106
RIP
authentication, basic configuration 115
basic configuration 107
configuring 109
explaining the RIP structure 110
how works 108
introduction 108
support 108
what is 108
RIP hold-down timer, what is 205
RIP structure, explanation 110
router
alarms 337
basic configuration 97
configuration attributes 200
general configuration attributes 201
general performance attributes 313
general status attributes 274
introduction 98
performance attributes 312
specifications 367
status attributes 273
router applications, introducing 5
routing
basic activities 98
determining the optimal path 98
static versus dynamic 99
transporting packets 98
versus bridging 98
what is 98
routing and bridging performance specifications 367
routing table, configuring the 102
routing traffic policy, applying on an interface 136

S

safety
compliance 368
instructions 14
requirements ii
sales codes 375
security
correcting the security table 63
selecting a site 16
self-learning bridge, what is 141
SNMP
configuration attributes 238

software
downloading 353
what is boot, loader and application 354

Spanning Tree
behaviour 146
bridge failure 146
bridging loops 146
network extension 146
BPDU 145
propagation of 145
what is 145
bridge port states 144
bridge priority, what is 147
path cost, example 148
path cost, what is 147
port priority, example 148
port priority, what is 147
priority and cost 147
root bridge 142
how selected 142
what is 142
topology 143

specifications
ATM encapsulation 366
auxiliary connector 365
bridging 367
control connector 364
dimensions 368
EMC compliance 368
environmental compliance 369
Frame Relay encapsulation 366
G703 interface 362
IP routing 367
LAN interface 363
over-voltage and over-current protection compliance 368
power requirements 368
PPP encapsulation 366
routing and bridging performance 367
safety compliance 368

statements iii

static routes
basic configuration 100, 101
examples 103
with IP address on the WAN 104
without IP address on the WAN 105

status attributes 245
ATM 270
bridge 287
default NAT 280
file system 294
Frame Relay 266
G703 channel 259
G703 interface 258
general 248
HDLC 272
L2TP tunnel 281
LAN interface 251
loop-back 293
management 293
operating system 296
overview 246
PPP 261
proxy 297
router 273
router, general 274
WAN interface 257

structured value, what is 42

T

technical specifications 361

Telindus 1030 Router series, what is 4

Time To Live (TTL), what is 209

TMA
connecting over an IP network 38
connecting through the control connector 36
how to connect 35
managing the device with 34
what is 35

TMA attribute string, reading a 54

TMA sub-system picture 339
how to display 339
structure 339

traffic and priority policy introduction 131

traffic and priority policy on routed and bridged data 132

traffic policy
configuration attributes 223
configuring an extended access list 138
configuring on the bridge 156
configuring on the router 134
how to configure on the bridge 155
how to configure on the router 133
what is 131

Transparent Spanning Tree bridge, what is 141

U

unpacking 15

using PAT over PPP with a minimum of official IP addresses, a configuration example 164

V

value, what is 42

VCI, what is 87

VPI, what is 87

W

WAN encapsulation
basic configuration 71

WAN interface
configuration attributes 181
performance attributes 305
status attributes 257

warning
EMC 17
ESD 17
important safety instructions 14
safety 14
selecting a site 16